

INTELLIGENCE COMMUNITY
LEGAL REFERENCE BOOK
DIGITAL EDITION



OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
OFFICE OF GENERAL COUNSEL

SUMMER 2024

INTRODUCTION

On behalf of the Director of National Intelligence, I am pleased to make available the Summer 2024 edition of the Intelligence Community Legal Reference Book. The Office of General Counsel updated the Reference Book to reflect legal developments since the 2020 edition and comments received from the Intelligence Community. Additionally, we are updating the online version of the reference book to include additional references, available at www.dni.gov/ogc , and will endeavor to keep the online version updated throughout the year.

The body of law contained in this collection provides the Intelligence Community with much of its authority and guidance. We hope this collection will provide professionals across the federal government with a helpful, consolidated resource to use in their day-to-day work on behalf of the American people.

This new edition is the result of many hours of hard work. I would like to extend my thanks to the Office of General Counsel team and those across the Community who assisted in recommending and preparing the authorities contained herein. I hope this book proves a valuable addition to your library and a useful tool as you carry out your vital mission.

Tricia Wellman
Acting General Counsel
Summer 2024

ABOUT THIS BOOK

The documents presented in this book have been updated to incorporate all amendments made since the Winter 2020 version through June 20, 2024, at which point the documents were, where possible, verified against the United States Code maintained by The Library of Congress and Westlaw. The text of these documents should be cited as “as amended.” Editorial notes throughout the book have been placed in brackets or otherwise noted.

All documents in this book are UNCLASSIFIED.

This compilation was a significant effort and required many judgments concerning what text to include and how to organize the book. We welcome your thoughts for improving future versions.

TABLE OF CONTENTS

Introduction.....	iii
Table of Contents.....	vii
THE CONSTITUTION OF THE UNITED STATES OF AMERICA	1
PRINCIPLES OF PROFESSIONAL ETHICS FOR THE INTELLIGENCE COMMUNITY	22
PRINCIPLES OF INTELLIGENCE TRANSPARENCY FOR THE INTELLIGENCE COMMUNITY	24
NATIONAL SECURITY ACT OF 1947	26
INTELLIGENCE REFORM AND TERRORISM PREVENTION ACT OF 2004	256
CENTRAL INTELLIGENCE AGENCY ACT OF 1949	286
NATIONAL SECURITY AGENCY ACT OF 1959.....	357
TITLE 10, UNITED STATES CODE, DEPARTMENT OF DEFENSE AUTHORITIES	372
TITLE 10, CHAPTER 22, UNITED STATES CODE, NATIONAL GEOSPATIAL- INTELLIGENCE AGENCY AUTHORITIES	389
HOMELAND SECURITY ACT OF 2002	400
COUNTERINTELLIGENCE AND SECURITY ENHANCEMENTS ACT OF 1994	466
COUNTERINTELLIGENCE ENHANCEMENT ACT OF 2002	470
CLASSIFIED INFORMATION PROCEDURES ACT	476
FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978.....	486
TITLE 5, SECTION 552, UNITED STATES CODE (THE “FREEDOM OF INFORMATION ACT”)	624
TITLE 5, SECTION 552A, UNITED STATES CODE (THE “PRIVACY ACT”)	648
WAR CRIMES ACT OF 1996	668
EXECUTIVE ORDER 12139: FOREIGN INTELLIGENCE ELECTRONIC SURVEILLANCE	680
EXECUTIVE ORDER 12333: UNITED STATES INTELLIGENCE ACTIVITIES	682
EXECUTIVE ORDER 12949: FOREIGN INTELLIGENCE PHYSICAL SEARCHES	709
EXECUTIVE ORDER 12968: ACCESS TO CLASSIFIED INFORMATION	711
EXECUTIVE ORDER 13388: FURTHER STRENGTHENING THE SHARING OF TERRORISM INFORMATION TO PROTECT AMERICANS	726
EXECUTIVE ORDER 13462: PRESIDENT’S INTELLIGENCE ADVISORY BOARD AND INTELLIGENCE OVERSIGHT BOARD	730
EXECUTIVE ORDER 13467: REFORMING PROCESSES RELATED TO SUITABILITY FOR GOVERNMENT EMPLOYMENT, FITNESS FOR CONTRACTOR EMPLOYEES, AND ELIGIBILITY FOR ACCESS TO CLASSIFIED NATIONAL SECURITY INFORMATION.....	736
EXECUTIVE ORDER 13491: ENSURING LAWFUL INTERROGATION.....	760
EXECUTIVE ORDER 13526: CLASSIFIED NATIONAL SECURITY INFORMATION	765
EXECUTIVE ORDER 13636: IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY.....	800

EXECUTIVE ORDER 14086: ENHANCING SAFEGUARDS FOR UNITED STATES SIGNALS INTELLIGENCE ACTIVITIES	809
NATIONAL SECURITY MEMORANDUM ON PARTIAL REVOCATION OF PRESIDENTIAL POLICY DIRECTIVE 28.....	832
PRESIDENTIAL POLICY DIRECTIVE – SIGNALS INTELLIGENCE ACTIVITIES	834
PRESIDENTIAL POLICY DIRECTIVE – PROTECTING WHISTLEBLOWERS WITH ACCESS TO CLASSIFIED INFORMATION.....	838
CRITERIA ON THRESHOLDS FOR REPORTING INTELLIGENCE OVERSIGHT MATTERS AND INSTRUCTIONS RELATING TO FORMATTING AND SCHEDULING	845
MEMORANDUM OF UNDERSTANDING: REPORTING OF INFORMATION CONCERNING FEDERAL CRIMES.....	849
INTELLIGENCE COMMUNITY AND GOVERNMENT WEBSITES	861
<u>PROCEDURES FOR THE RETENTION OF INCIDENTALLY ACQUIRED COMMUNICATIONS</u>	864
<u>TITLE 10, CHAPTER 47A, UNITED STATES CODE, MILITARY COMMISSIONS</u>	867
<u>E-GOVERNMENT ACT OF 2002</u>	919
<u>FEDERAL AGENCY DATA MINING REPORTING ACT OF 2007</u>	924
<u>FEDERAL INFORMATION SECURITY MODERNIZATION ACT [FISMA] OF 2014</u>	927
<u>TITLE 40, CHAPTER 113, UNITED STATES CODE, RESPONSIBILITIES FOR FEDERAL INFORMATION SYSTEMS STANDARDS</u>	947
<u>CYBERSECURITY ACT OF 2015</u>	949
<u>AI ETHICS FRAMEWORK FOR THE INTELLIGENCE COMMUNITY</u>	984
<u>INTELLIGENCE SHARING PROCEDURES FOR FOREIGN INTELLIGENCE AND FOREIGN COUNTERINTELLIGENCE INVESTIGATIONS CONDUCTED BY THE FEDERAL BUREAU OF INVESTIGATION</u>	992
<u>GUIDELINES REGARDING DISCLOSURE TO THE DIRECTOR OF CENTRAL INTELLIGENCE AND HOMELAND SECURITY OFFICIALS OF FOREIGN INTELLIGENCE ACQUIRED IN THE COURSE OF A CRIMINAL INVESTIGATION</u>	998
<u>GUIDELINES REGARDING PROMPT HANDLING OF REPORTS OF POSSIBLE CRIMINAL ACTIVITY INVOLVING FOREIGN INTELLIGENCE SOURCES</u>	1006
<u>GUIDELINES TO ENSURE THAT THE INFORMATION PRIVACY AND OTHER LEGAL RIGHTS OF AMERICANS ARE PROTECTED IN THE DEVELOPMENT AND USE OF THE INFORMATION SHARING ENVIRONMENT</u>	1009
<u>MEMORANDUM ON IMPROVING THE CYBERSECURITY OF NATIONAL SECURITY, DEPARTMENT OF DEFENSE, AND INTELLIGENCE COMMUNITY SYSTEMS</u>	1017
<u>TITLE 44, SECTION 3520, UNITED STATES CODE</u>	1029
<u>TITLE 10, SECTION 431, UNITED STATES CODE</u>	1031
<u>TITLE 18, SECTION 2703, UNITED STATES CODE (THE “STORED COMMUNICATIONS ACT”)</u>	1032
<u>TITLE 18, SECTION 2709, UNITED STATES CODE (THE “STORED COMMUNICATIONS ACT”)</u>	1038

TITLE 12, SECTION 3414, UNITED STATES CODE (THE “RIGHT TO FINANCIAL PRIVACY ACT”).....1041
TITLE 15, SECTION 1681u, UNITED STATES CODE (THE “FAIR CREDIT REPORTING ACT”).....1046
TITLE 28, SECTION 0.85, CODE OF FEDERAL REGULATIONS1051
TITLE 10, SECTION 431, UNITED STATES CODE1054
TITLE 18, SECTION 1030, UNITED STATES CODE.....1055
TITLE 28, SECTION 533, UNITED STATES CODE1063

THE CONSTITUTION OF THE UNITED STATES OF AMERICA

PREAMBLE

We the People of the United States, in Order to form a more perfect Union, establish Justice, insure domestic Tranquility, provide for the common defense, promote the general Welfare, and secure the Blessings of Liberty to ourselves and our Posterity, do ordain and establish this Constitution for the United States of America.

ARTICLE. I.

SECTION 1.

All legislative Powers herein granted shall be vested in a Congress of the United States, which shall consist of a Senate and House of Representatives.

SECTION 2.

The House of Representatives shall be composed of Members chosen every second Year by the People of the several States, and the Electors in each State shall have the Qualifications requisite for Electors of the most numerous Branch of the State Legislature.

No Person shall be a Representative who shall not have attained to the Age of twenty five Years, and been seven Years a Citizen of the United States, and who shall not, when elected, be an Inhabitant of that State in which he shall be chosen.

Representatives and direct Taxes shall be apportioned among the several States which may be included within this Union, according to their respective Numbers, which shall be determined by adding to the whole Number of free Persons, including those bound to Service for a Term of Years, and excluding Indians not taxed, three fifths of all other Persons. The actual Enumeration shall be made within three Years after the first Meeting of the Congress of the United States, and within every subsequent Term of ten Years, in such Manner as they shall by Law direct. The Number of Representatives shall not exceed one for every thirty Thousand, but each State shall have at Least one Representative; and until such enumeration shall be made, the State of New Hampshire shall be entitled to chuse three, Massachusetts eight, Rhode-Island and Providence Plantations one, Connecticut five, New-York six, New Jersey four, Pennsylvania eight, Delaware one, Maryland six, Virginia ten, North Carolina five, South Carolina five, and Georgia three.

UNITED STATES CONSTITUTION

When vacancies happen in the Representation from any State, the Executive Authority thereof shall issue Writs of Election to fill such Vacancies.

The House of Representatives shall chuse their Speaker and other Officers; and shall have the sole Power of Impeachment.

SECTION 3.

The Senate of the United States shall be composed of two Senators from each State, chosen by the Legislature thereof, for six Years; and each Senator shall have one Vote.

Immediately after they shall be assembled in Consequence of the first Election, they shall be divided as equally as may be into three Classes. The Seats of the Senators of the first Class shall be vacated at the Expiration of the second Year, of the second Class at the Expiration of the fourth Year, and of the third Class at the Expiration of the sixth Year, so that one third may be chosen every second Year; and if Vacancies happen by Resignation, or otherwise, during the Recess of the Legislature of any State, the Executive thereof may make temporary Appointments until the next Meeting of the Legislature, which shall then fill such Vacancies.

No Person shall be a Senator who shall not have attained to the Age of thirty Years, and been nine Years a Citizen of the United States, and who shall not, when elected, be an Inhabitant of that State for which he shall be chosen.

The Vice President of the United States shall be President of the Senate but shall have no Vote, unless they be equally divided.

The Senate shall chuse their other Officers, and also a President pro tempore, in the Absence of the Vice President, or when he shall exercise the Office of President of the United States.

The Senate shall have the sole Power to try all Impeachments. When sitting for that Purpose, they shall be on Oath or Affirmation. When the President of the United States is tried, the Chief Justice shall preside: And no Person shall be convicted without the Concurrence of two thirds of the Members present.

Judgment in Cases of Impeachment shall not extend further than to removal from Office, and disqualification to hold and enjoy any Office of honor, Trust or Profit under the United States: but the Party convicted shall nevertheless be liable and subject to Indictment, Trial, Judgment and Punishment, according to Law.

SECTION 4.

The Times, Places and Manner of holding Elections for Senators and Representatives, shall be prescribed in each State by the Legislature thereof; but the Congress may at any time by Law make or alter such Regulations, except as to the Places of chusing Senators.

The Congress shall assemble at least once in every Year, and such Meeting shall be on the first Monday in December, unless they shall by Law appoint a different Day.

SECTION 5.

Each House shall be the Judge of the Elections, Returns and Qualifications of its own Members, and a Majority of each shall constitute a Quorum to do Business; but a smaller Number may adjourn from day to day, and may be authorized to compel the Attendance of absent Members, in such Manner, and under such Penalties as each House may provide.

Each House may determine the Rules of its Proceedings, punish its Members for disorderly Behaviour, and, with the Concurrence of two thirds, expel a Member.

Each House shall keep a Journal of its Proceedings, and from time to time publish the same, excepting such Parts as may in their Judgment require Secrecy; and the Yeas and Nays of the Members of either House on any question shall, at the Desire of one fifth of those Present, be entered on the Journal.

Neither House, during the Session of Congress, shall, without the Consent of the other, adjourn for more than three days, nor to any other Place than that in which the two Houses shall be sitting.

SECTION 6.

The Senators and Representatives shall receive a Compensation for their Services, to be ascertained by Law, and paid out of the Treasury of the United States. They shall in all Cases, except Treason, Felony and Breach of the Peace, be privileged from Arrest during their Attendance at the Session of their respective Houses, and in going to and returning from the same; and for any Speech or Debate in either House, they shall not be questioned in any other Place.

No Senator or Representative shall, during the Time for which he was elected, be appointed to any civil Office under the Authority of the United States, which shall have been created, or the Emoluments whereof shall have been increased

during such time; and no Person holding any Office under the United States, shall be a Member of either House during his Continuance in Office.

SECTION 7.

All Bills for raising Revenue shall originate in the House of Representatives; but the Senate may propose or concur with Amendments as on other Bills.

Every Bill which shall have passed the House of Representatives and the Senate, shall, before it become a law, be presented to the President of the United States: If he approve he shall sign it, but if not he shall return it, with his Objections to that House in which it shall have originated, who shall enter the Objections at large on their Journal, and proceed to reconsider it. If after such Reconsideration two thirds of that House shall agree to pass the Bill, it shall be sent, together with the Objections, to the other House, by which it shall likewise be reconsidered, and if approved by two thirds of that House, it shall become a Law. But in all such Cases the Votes of both Houses shall be determined by Yeas and Nays, and the Names of the Persons voting for and against the Bill shall be entered on the Journal of each House respectively. If any Bill shall not be returned by the President within ten Days (Sundays excepted) after it shall have been presented to him, the Same shall be a Law, in like Manner as if he had signed it, unless the Congress by their Adjournment prevent its Return, in which Case it shall not be a Law.

Every Order, Resolution, or Vote to which the Concurrence of the Senate and House of Representatives may be necessary (except on a question of Adjournment) shall be presented to the President of the United States; and before the Same shall take Effect, shall be approved by him, or being disapproved by him, shall be repassed by two thirds of the Senate and House of Representatives, according to the Rules and Limitations prescribed in the Case of a Bill.

SECTION 8.

The Congress shall have Power To lay and collect Taxes, Duties, Imposts and Excises, to pay the Debts and provide for the common Defence and general Welfare of the United States; but all Duties, Imposts and Excises shall be uniform throughout the United States;

To borrow Money on the credit of the United States;

To regulate Commerce with foreign Nations, and among the several States, and with the Indian Tribes;

UNITED STATES CONSTITUTION

To establish an uniform Rule of Naturalization, and uniform Laws on the subject of Bankruptcies throughout the United States;

To coin Money, regulate the Value thereof, and of foreign Coin, and fix the Standard of Weights and Measures;

To provide for the Punishment of counterfeiting the Securities and current Coin of the United States;

To establish Post Offices and post Roads;

To promote the Progress of Science and useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries;

To constitute Tribunals inferior to the supreme Court;

To define and punish Piracies and Felonies committed on the high Seas, and Offences against the Law of Nations;

To declare War, grant Letters of Marque and Reprisal, and make Rules concerning Captures on Land and Water;

To raise and support Armies, but no Appropriation of Money to that Use shall be for a longer Term than two Years;

To provide and maintain a Navy;

To make Rules for the Government and Regulation of the land and naval Forces;

To provide for calling forth the Militia to execute the Laws of the Union, suppress Insurrections and repel Invasions;

To provide for organizing, arming, and disciplining, the Militia, and for governing such Part of them as may be employed in the Service of the United States, reserving to the States respectively, the Appointment of the Officers, and the Authority of training the Militia according to the discipline prescribed by Congress;

To exercise exclusive Legislation in all Cases whatsoever, over such District (not exceeding ten Miles square) as may, by Cession of particular States, and the

UNITED STATES CONSTITUTION

Acceptance of Congress, become the Seat of the Government of the United States, and to exercise like Authority over all Places purchased by the Consent of the Legislature of the State in which the Same shall be, for the Erection of Forts, Magazines, Arsenals, dock-Yards, and other needful Buildings;—And

To make all Laws which shall be necessary and proper for carrying into Execution the foregoing Powers, and all other Powers vested by this Constitution in the Government of the United States, or in any Department or Officer thereof.

SECTION 9.

The Migration or Importation of such Persons as any of the States now existing shall think proper to admit, shall not be prohibited by the Congress prior to the Year one thousand eight hundred and eight, but a Tax or duty may be imposed on such Importation, not exceeding ten dollars for each Person.

The Privilege of the Writ of Habeas Corpus shall not be suspended, unless when in Cases of Rebellion or Invasion the public Safety may require it.

No Bill of Attainder or ex post facto Law shall be passed.

No Capitation, or other direct, Tax shall be laid, unless in Proportion to the Census or Enumeration herein before directed to be taken.

No Tax or Duty shall be laid on Articles exported from any State.

No Preference shall be given by any Regulation of Commerce or Revenue to the Ports of one State over those of another: nor shall Vessels bound to, or from, one State, be obliged to enter, clear, or pay Duties in another.

No Money shall be drawn from the Treasury, but in Consequence of Appropriations made by Law; and a regular Statement and Account of the Receipts and Expenditures of all public Money shall be published from time to time.

No Title of Nobility shall be granted by the United States: And no Person holding any Office of Profit or Trust under them, shall, without the Consent of the Congress, accept of any present, Emolument, Office, or Title, of any kind whatever, from any King, Prince or foreign State.

SECTION 10.

No State shall enter into any Treaty, Alliance, or Confederation; grant Letters of Marque and Reprisal; coin Money; emit Bills of Credit; make any Thing but gold and silver Coin a Tender in Payment of Debts; pass any Bill of Attainder, ex post facto Law, or Law impairing the Obligation of Contracts, or grant any Title of Nobility.

No State shall, without the Consent of the Congress, lay any Imposts or Duties on Imports or Exports, except what may be absolutely necessary for executing it's inspection Laws: and the net Produce of all Duties and Imposts, laid by any State on Imports or Exports, shall be for the Use of the Treasury of the United States; and all such Laws shall be subject to the Revision and Controul of the Congress.

No State shall, without the Consent of Congress, lay any Duty of Tonnage, keep Troops, or Ships of War in time of Peace, enter into any Agreement or Compact with another State, or with a foreign Power, or engage in War, unless actually invaded, or in such imminent Danger as will not admit of delay.

ARTICLE. II.

SECTION 1.

The executive Power shall be vested in a President of the United States of America. He shall hold his Office during the Term of four Years, and, together with the Vice President, chosen for the same Term, be elected, as follows:

Each State shall appoint, in such Manner as the Legislature thereof may direct, a Number of Electors, equal to the whole Number of Senators and Representatives to which the State may be entitled in the Congress: but no Senator or Representative, or Person holding an Office of Trust or Profit under the United States, shall be appointed an Elector.

The Electors shall meet in their respective States, and vote by Ballot for two Persons, of whom one at least shall not be an Inhabitant of the same State with themselves. And they shall make a List of all the Persons voted for, and of the Number of Votes for each; which List they shall sign and certify, and transmit sealed to the Seat of the Government of the United States, directed to the President of the Senate. The President of the Senate shall, in the Presence of the Senate and House of Representatives, open all the Certificates, and the Votes shall then be counted. The Person having the greatest Number of Votes shall be the President, if such Number be a Majority of the whole Number of Electors appointed; and if there be more than one who have such Majority, and have an equal Number of Votes, then the House of Representatives shall immediately

UNITED STATES CONSTITUTION

chuse by Ballot one of them for President; and if no Person have a Majority, then from the five highest on the List the said House shall in like Manner chuse the President. But in chusing the President, the Votes shall be taken by States, the Representatives from each State having one Vote; a quorum for this Purpose shall consist of a Member or Members from two thirds of the States, and a Majority of all the States shall be necessary to a Choice. In every Case, after the Choice of the President, the Person having the greatest Number of Votes of the Electors shall be the Vice President. But if there should remain two or more who have equal Votes, the Senate shall chuse from them by Ballot the Vice President.

The Congress may determine the Time of chusing the Electors, and the Day on which they shall give their Votes; which Day shall be the same throughout the United States.

No Person except a natural born Citizen, or a Citizen of the United States, at the time of the Adoption of this Constitution, shall be eligible to the Office of President; neither shall any person be eligible to that Office who shall not have attained to the Age of thirty five Years, and been fourteen Years a Resident within the United States.

In Case of the Removal of the President from Office, or of his Death, Resignation, or Inability to discharge the Powers and Duties of the said Office, the Same shall devolve on the Vice President, and the Congress may by Law provide for the Case of Removal, Death, Resignation or Inability, both of the President and Vice President, declaring what Officer shall then act as President, and such Officer shall act accordingly, until the Disability be removed, or a President shall be elected.

The President shall, at stated Times, receive for his Services, a Compensation, which shall neither be encreased nor diminished during the Period for which he shall have been elected, and he shall not receive within that Period any other Emolument from the United States, or any of them.

Before he enter on the Execution of his Office, he shall take the following Oath or Affirmation:—"I do solemnly swear (or affirm) that I will faithfully execute the Office of President of the United States, and will to the best of my Ability, preserve, protect and defend the Constitution of the United States."

SECTION 2.

The President shall be Commander in Chief of the Army and Navy of the United States, and of the Militia of the several States, when called into the actual Service

UNITED STATES CONSTITUTION

of the United States; he may require the Opinion, in writing, of the principal Officer in each of the executive Departments, upon any Subject relating to the Duties of their respective Offices, and he shall have Power to Grant Reprieves and Pardons for Offences against the United States, except in Cases of Impeachment.

He shall have Power, by and with the Advice and Consent of the Senate, to make Treaties, provided two thirds of the Senators present concur; and he shall nominate, and by and with the Advice and Consent of the Senate, shall appoint Ambassadors, other public Ministers and Consuls, Judges of the supreme Court, and all other Officers of the United States, whose Appointments are not herein otherwise provided for, and which shall be established by Law: but the Congress may by Law vest the Appointment of such inferior Officers, as they think proper, in the President alone, in the Courts of Law, or in the Heads of Departments.

The President shall have Power to fill up all Vacancies that may happen during the Recess of the Senate, by granting Commissions which shall expire at the End of their next Session.

SECTION 3.

He shall from time to time give to the Congress Information on the State of the Union, and recommend to their Consideration such Measures as he shall judge necessary and expedient; he may, on extraordinary Occasions, convene both Houses, or either of them, and in Case of Disagreement between them, with Respect to the Time of Adjournment, he may adjourn them to such Time as he shall think proper; he shall receive Ambassadors and other public Ministers; he shall take Care that the Laws be faithfully executed, and shall Commission all the Officers of the United States.

SECTION 4.

The President, Vice President and all Civil Officers of the United States, shall be removed from Office on Impeachment for, and Conviction of, Treason, Bribery, or other high Crimes and Misdemeanors.

ARTICLE. III.

SECTION 1.

The judicial Power of the United States, shall be vested in one supreme Court, and in such inferior Courts as the Congress may from time to time ordain and establish. The Judges, both of the supreme and inferior Courts, shall hold their Offices during good Behaviour, and shall, at stated Times, receive for their Services, a Compensation, which shall not be diminished during their Continuance in Office.

SECTION 2.

The judicial Power shall extend to all Cases, in Law and Equity, arising under this Constitution, the Laws of the United States, and Treaties made, or which shall be made, under their Authority;—to all Cases affecting Ambassadors, other public ministers and Consuls;—to all Cases of admiralty and maritime Jurisdiction;—to Controversies to which the United States shall be a Party;—to Controversies between two or more States;—between a State and Citizens of another State;—between Citizens of different States;—between Citizens of the same State claiming Lands under Grants of different States, and between a State, or the Citizens thereof, and foreign States, Citizens or Subjects.

In all Cases affecting Ambassadors, other public Ministers and Consuls, and those in which a State shall be Party, the supreme Court shall have original Jurisdiction. In all the other Cases before mentioned, the supreme Court shall have appellate Jurisdiction, both as to Law and Fact, with such Exceptions, and under such Regulations as the Congress shall make.

The Trial of all Crimes, except in Cases of Impeachment, shall be by Jury; and such Trial shall be held in the State where the said Crimes shall have been committed; but when not committed within any State, the Trial shall be at such Place or Places as the Congress may by Law have directed.

SECTION 3.

Treason against the United States, shall consist only in levying War against them, or in adhering to their Enemies, giving them Aid and Comfort. No Person shall be convicted of Treason unless on the Testimony of two Witnesses to the same overt Act, or on Confession in open Court.

The Congress shall have Power to declare the Punishment of Treason, but no Attainder of Treason shall work Corruption of Blood, or Forfeiture except during the Life of the Person attainted.

ARTICLE. IV.

SECTION 1.

Full Faith and Credit shall be given in each State to the public Acts, Records, and judicial Proceedings of every other State. And the Congress may by general Laws prescribe the Manner in which such Acts, Records and Proceedings shall be proved, and the Effect thereof.

UNITED STATES CONSTITUTION

SECTION 2.

The Citizens of each State shall be entitled to all Privileges and Immunities of Citizens in the several States.

A Person charged in any State with Treason, Felony, or other Crime, who shall flee from Justice, and be found in another State, shall on Demand of the executive Authority of the State from which he fled, be delivered up, to be removed to the State having Jurisdiction of the Crime.

No Person held to Service or Labour in one State, under the Laws thereof, escaping into another, shall, in Consequence of any Law or Regulation therein, be discharged from such Service or Labour, but shall be delivered up on Claim of the Party to whom such Service or Labour may be due.

SECTION 3.

New States may be admitted by the Congress into this Union; but no new State shall be formed or erected within the Jurisdiction of any other State; nor any State be formed by the Junction of two or more States, or Parts of States, without the Consent of the Legislatures of the States concerned as well as of the Congress.

The Congress shall have Power to dispose of and make all needful Rules and Regulations respecting the Territory or other Property belonging to the United States; and nothing in this Constitution shall be so construed as to Prejudice any Claims of the United States, or of any particular State.

SECTION 4.

The United States shall guarantee to every State in this Union a Republican Form of Government, and shall protect each of them against Invasion; and on Application of the Legislature, or of the Executive (when the Legislature cannot be convened) against domestic Violence.

ARTICLE. V.

The Congress, whenever two thirds of both Houses shall deem it necessary, shall propose Amendments to this Constitution, or, on the Application of the Legislatures of two thirds of the several States, shall call a Convention for proposing Amendments, which, in either Case, shall be valid to all Intents and Purposes, as Part of this Constitution, when ratified by the Legislatures of three fourths of the several States, or by Conventions in three fourths thereof, as the one or the other Mode of Ratification may be proposed by the Congress;

UNITED STATES CONSTITUTION

Provided that no Amendment which may be made prior to the Year One thousand eight hundred and eight shall in any Manner affect the first and fourth Clauses in the Ninth Section of the first Article; and that no State, without its Consent, shall be deprived of its equal Suffrage in the Senate.

ARTICLE. VI.

All Debts contracted and Engagements entered into, before the Adoption of this Constitution, shall be as valid against the United States under this Constitution, as under the Confederation.

This Constitution, and the Laws of the United States which shall be made in Pursuance thereof; and all Treaties made, or which shall be made, under the Authority of the United States, shall be the supreme Law of the Land; and the Judges in every State shall be bound thereby, any Thing in the Constitution or Laws of any state to the Contrary notwithstanding.

The Senators and Representatives before mentioned, and the Members of the several State Legislatures, and all executive and judicial Officers, both of the United States and of the several States, shall be bound by Oath or Affirmation, to support this Constitution; but no religious Test shall ever be required as a Qualification to any Office or public Trust under the United States.

ARTICLE. VII.

The Ratification of the Conventions of nine States, shall be sufficient for the Establishment of this Constitution between the States so ratifying the Same.

AMENDMENT I.

Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances.

AMENDMENT II.

A well regulated Militia, being necessary to the security of a free State, the right of the people to keep and bear Arms, shall not be infringed.

UNITED STATES CONSTITUTION

AMENDMENT III.

No Soldier shall, in time of peace be quartered in any house, without the consent of the Owner, nor in time of war, but in a manner to be prescribed by law.

AMENDMENT IV.

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

AMENDMENT V.

No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a Grand Jury, except in cases arising in the land or naval forces, or in the Militia, when in actual service in time of War or public danger; nor shall any person be subject for the same offence to be twice put in jeopardy of life or limb; nor shall be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation.

AMENDMENT VI.

In all criminal prosecutions, the accused shall enjoy the right to a speedy and public trial, by an impartial jury of the State and district wherein the crime shall have been committed, which district shall have been previously ascertained by law, and to be informed of the nature and cause of the accusation; to be confronted with the witnesses against him; to have compulsory process for obtaining witnesses in his favor, and to have the Assistance of Counsel for his defence.

AMENDMENT VII.

In Suits at common law, where the value in controversy shall exceed twenty dollars, the right of trial by jury shall be preserved, and no fact tried by a jury, shall be otherwise re-examined in any Court of the United States, than according to the rules of the common law.

UNITED STATES CONSTITUTION

AMENDMENT VIII.

Excessive bail shall not be required, nor excessive fines imposed, nor cruel and unusual punishments inflicted.

AMENDMENT IX.

The enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people.

AMENDMENT X.

The powers not delegated to the United States by the Constitution, nor prohibited by it to the States, are reserved to the States respectively, or to the people.

AMENDMENT XI.

The Judicial power of the United States shall not be construed to extend to any suit in law or equity, commenced or prosecuted against one of the United States by Citizens of another State, or by Citizens or Subjects of any Foreign State.

AMENDMENT XII.

The Electors shall meet in their respective states and vote by ballot for President and Vice-President, one of whom, at least, shall not be an inhabitant of the same state with themselves; they shall name in their ballots the person voted for as President, and in distinct ballots the person voted for as Vice- President, and they shall make distinct lists of all persons voted for as President, and of all persons voted for as Vice-President, and of the number of votes for each, which lists they shall sign and certify, and transmit sealed to the seat of the government of the United States, directed to the President of the Senate;—The President of the Senate shall, in the presence of the Senate and House of Representatives, open all the certificates and the votes shall then be counted;—The person having the greatest Number of votes for President, shall be the President, if such number be a majority of the whole number of Electors appointed; and if no person have such majority, then from the persons having the highest numbers not exceeding three on the list of those voted for as President, the House of Representatives shall choose immediately, by ballot, the President. But in choosing the President, the votes shall be taken by states, the representation from each state having one vote; a quorum for this purpose shall consist of a member or members from two-thirds of the states, and a majority of all the states shall be necessary to a choice. And if

UNITED STATES CONSTITUTION

the House of Representatives shall not choose a President whenever the right of choice shall devolve upon them, before the fourth day of March next following, then the Vice- President shall act as President, as in the case of the death or other constitutional disability of the President—The person having the greatest number of votes as Vice-President, shall be the Vice-President, if such number be a majority of the whole number of Electors appointed, and if no person have a majority, then from the two highest numbers on the list, the Senate shall choose the Vice-President; a quorum for the purpose shall consist of two-thirds of the whole number of Senators, and a majority of the whole number shall be necessary to a choice. But no person constitutionally ineligible to the office of President shall be eligible to that of Vice-President of the United States.

AMENDMENT XIII.

SECTION. 1. Neither slavery nor involuntary servitude, except as a punishment for crime whereof the party shall have been duly convicted, shall exist within the United States, or any place subject to their jurisdiction.

SECTION. 2. Congress shall have power to enforce this article by appropriate legislation.

AMENDMENT XIV.

SECTION. 1. All persons born or naturalized in the United States and subject to the jurisdiction thereof, are citizens of the United States and of the State wherein they reside. No State shall make or enforce any law which shall abridge the privileges or immunities of citizens of the United States; nor shall any State deprive any person of life, liberty, or property, without due process of law; nor deny to any person within its jurisdiction the equal protection of the laws.

SECTION. 2. Representatives shall be apportioned among the several States according to their respective numbers, counting the whole number of persons in each State, excluding Indians not taxed. But when the right to vote at any election for the choice of electors for President and Vice President of the United States, Representatives in Congress, the Executive and Judicial officers of a State, or the members of the Legislature thereof, is denied to any of the male inhabitants of such State, being twenty-one years of age, and citizens of the United States, or in any way abridged, except for participation in rebellion, or other crime, the basis of representation therein shall be reduced in the proportion which the number of such male citizens shall bear to the whole number of male citizens twenty-one years of age in such State.

UNITED STATES CONSTITUTION

SECTION. 3. No person shall be a Senator or Representative in Congress, or elector of President and Vice President, or hold any office, civil or military, under the United States, or under any State, who, having previously taken an oath, as a member of Congress, or as an officer of the United States, or as a member of any State legislature, or as an executive or judicial officer of any State, to support the Constitution of the United States, shall have engaged in insurrection or rebellion against the same, or given aid or comfort to the enemies thereof. But Congress may by a vote of two-thirds of each House, remove such disability.

SECTION. 4. The validity of the public debt of the United States, authorized by law, including debts incurred for payment of pensions and bounties for services in suppressing insurrection or rebellion, shall not be questioned. But neither the United States nor any State shall assume or pay any debt or obligation incurred in aid of insurrection or rebellion against the United States, or any claim for the loss or emancipation of any slave; but all such debts, obligations and claims shall be held illegal and void.

SECTION. 5. The Congress shall have power to enforce, by appropriate legislation, the provisions of this article.

AMENDMENT XVII.

SECTION. 1. The right of citizens of the United States to vote shall not be denied or abridged by the United States or by any State on account of race, color, or previous condition of servitude.

SECTION. 2. The Congress shall have power to enforce this article by appropriate legislation.

AMENDMENT XVI.

The Congress shall have power to lay and collect taxes on incomes, from whatever source derived, without apportionment among the several States, and without regard to any census or enumeration.

AMENDMENT XVII.

The Senate of the United States shall be composed of two Senators from each State, elected by the people thereof, for six years; and each Senator shall have

UNITED STATES CONSTITUTION

one vote. The electors in each State shall have the qualifications requisite for electors of the most numerous branch of the State legislatures.

When vacancies happen in the representation of any State in the Senate, the executive authority of such State shall issue writs of election to fill such vacancies: Provided, That the legislature of any State may empower the executive thereof to make temporary appointments until the people fill the vacancies by election as the legislature may direct.

This amendment shall not be so construed as to affect the election or term of any Senator chosen before it becomes valid as part of the Constitution.

AMENDMENT XVIII.

SECTION. 1. After one year from the ratification of this article the manufacture, sale, or transportation of intoxicating liquors within, the importation thereof into, or the exportation thereof from the United States and all territory subject to the jurisdiction thereof for beverage purposes is hereby prohibited.

SECTION. 2. The Congress and the several States shall have concurrent power to enforce this article by appropriate legislation.

SECTION. 3. This article shall be inoperative unless it shall have been ratified as an amendment to the Constitution by the legislatures of the several States, as provided in the Constitution, within seven years from the date of the submission hereof to the States by the Congress.

AMENDMENT XIX.

The right of citizens of the United States to vote shall not be denied or abridged by the United States or by any State on account of sex.

Congress shall have power to enforce this article by appropriate legislation.

AMENDMENT XX.

SECTION. 1. The terms of the President and Vice President shall end at noon on the 20th day of January, and the terms of Senators and Representatives at noon on the 3d day of January, of the years in which such terms would have ended if this article had not been ratified; and the terms of their successors shall then begin.

UNITED STATES CONSTITUTION

SECTION. 2. The Congress shall assemble at least once in every year, and such meeting shall begin at noon on the 3d day of January, unless they shall by law appoint a different day.

SECTION. 3. If, at the time fixed for the beginning of the term of the President, the President elect shall have died, the Vice President elect shall become President. If a President shall not have been chosen before the time fixed for the beginning of his term, or if the President elect shall have failed to qualify, then the Vice President elect shall act as President until a President shall have qualified; and the Congress may by law provide for the case wherein neither a President elect nor a Vice President elect shall have qualified, declaring who shall then act as President, or the manner in which one who is to act shall be selected, and such person shall act accordingly until a President or Vice President shall have qualified.

SECTION. 4. The Congress may by law provide for the case of the death of any of the persons from whom the House of Representatives may choose a President whenever the right of choice shall have devolved upon them, and for the case of the death of any of the persons from whom the Senate may choose a Vice President whenever the right of choice shall have devolved upon them.

SECTION. 5. Sections 1 and 2 shall take effect on the 15th day of October following the ratification of this article.

SECTION. 6. This article shall be inoperative unless it shall have been ratified as an amendment to the Constitution by the legislatures of three-fourths of the several States within seven years from the date of its submission.

AMENDMENT XXI.

SECTION. 1. The eighteenth article of amendment to the Constitution of the United States is hereby repealed.

SECTION. 2. The transportation or importation into any State, Territory, or possession of the United States for delivery or use therein of intoxicating liquors, in violation of the laws thereof, is hereby prohibited.

SECTION. 3. This article shall be inoperative unless it shall have been ratified as an amendment to the Constitution by conventions in the several States, as provided in the Constitution, within seven years from the date of the submission hereof to the States by the Congress.

UNITED STATES CONSTITUTION

AMENDMENT XXII.

SECTION. 1. No person shall be elected to the office of the President more than twice, and no person who has held the office of President, or acted as President, for more than two years of a term to which some other person was elected President shall be elected to the office of the President more than once. But this Article shall not apply to any person holding the office of President, when this Article was proposed by the Congress, and shall not prevent any person who may be holding the office of President, or acting as President, during the term within which this Article becomes operative from holding the office of President or acting as President during the remainder of such term.

SECTION. 2. This article shall be inoperative unless it shall have been ratified as an amendment to the Constitution by the legislatures of three-fourths of the several States within seven years from the date of its submission to the States by the Congress.

AMENDMENT XXIII.

SECTION. 1. The District constituting the seat of Government of the United States shall appoint in such manner as the Congress may direct:

A number of electors of President and Vice President equal to the whole number of Senators and Representatives in Congress to which the District would be entitled if it were a State, but in no event more than the least populous State; they shall be in addition to those appointed by the States, but they shall be considered, for the purposes of the election of President and Vice President, to be electors appointed by a State; and they shall meet in the District and perform such duties as provided by the twelfth article of amendment.

SECTION. 2. The Congress shall have power to enforce this article by appropriate legislation.

AMENDMENT XXIV.

SECTION. 1. The right of citizens of the United States to vote in any primary or other election for President or Vice President, for electors for President or Vice President, or for Senator or Representative in Congress, shall not be denied or abridged by the United States or any State by reason of failure to pay any poll tax or other tax.

UNITED STATES CONSTITUTION

SECTION. 2. The Congress shall have power to enforce this article by appropriate legislation.

AMENDMENT XXV.

SECTION. 1. In case of the removal of the President from office or of his death or resignation, the Vice President shall become President.

SECTION. 2. Whenever there is a vacancy in the office of the Vice President, the President shall nominate a Vice President who shall take office upon confirmation by a majority vote of both Houses of Congress.

SECTION. 3. Whenever the President transmits to the President pro tempore of the Senate and the Speaker of the House of Representatives his written declaration that he is unable to discharge the powers and duties of his office, and until he transmits to them a written declaration to the contrary, such powers and duties shall be discharged by the Vice President as Acting President.

SECTION. 4. Whenever the Vice President and a majority of either the principal officers of the executive departments or of such other body as Congress may by law provide, transmit to the President pro tempore of the Senate and the Speaker of the House of Representatives their written declaration that the President is unable to discharge the powers and duties of his office, the Vice President shall immediately assume the powers and duties of the office as Acting President.

Thereafter, when the President transmits to the President pro tempore of the Senate and the Speaker of the House of Representatives his written declaration that no inability exists, he shall resume the powers and duties of his office unless the Vice President and a majority of either the principal officers of the executive department or of such other body as Congress may by law provide, transmit within four days to the President pro tempore of the Senate and the Speaker of the House of Representatives their written declaration that the President is unable to discharge the powers and duties of his office. Thereupon Congress shall decide the issue, assembling within forty-eight hours for that purpose if not in session. If the Congress, within twenty-one days after receipt of the latter written declaration, or, if Congress is not in session, within twenty-one days after Congress is required to assemble, determines by two-thirds vote of both Houses that the President is unable to discharge the powers and duties of his office, the Vice President shall continue to discharge the same as Acting President; otherwise, the President shall resume the powers and duties of his office.

UNITED STATES CONSTITUTION

AMENDMENT XXVI.

SECTION. 1. The right of citizens of the United States, who are eighteen years of age or older, to vote shall not be denied or abridged by the United States or by any State on account of age.

Section. 2. The Congress shall have power to enforce this article by appropriate legislation.

AMENDMENT XXVII.

No law varying the compensation for the services of the Senators and Representatives shall take effect, until an election of Representatives shall have intervened.

**PRINCIPLES OF PROFESSIONAL ETHICS FOR THE INTELLIGENCE
COMMUNITY**

As members of the intelligence profession, we conduct ourselves in accordance with certain basic principles. These principles are stated below, and reflect the standard of ethical conduct expected of all Intelligence Community personnel, regardless of individual role or agency affiliation.

Many of these principles are also reflected in other documents that we look to for guidance, such as statements of core values, and the Code of Conduct: Principles of Ethical Conduct for Government Officers and Employees; it is nonetheless important for the Intelligence Community to set forth in a single statement the fundamental ethical principles that unite us – and distinguish us – as intelligence professionals.

MISSION

We serve the American people, and understand that our mission requires selfless dedication to the security of our Nation.

TRUTH

We seek the truth; speak truth to power; and obtain, analyze, and provide intelligence objectively.

LAWFULNESS

We support and defend the Constitution, and comply with the laws of the United States, ensuring that we carry out our mission in a manner that respects privacy, civil liberties, and human rights obligations.

INTEGRITY

We demonstrate integrity in our conduct, mindful that all our actions, whether public or not, should reflect positively on the Intelligence Community at large.

STEWARDSHIP

We are responsible stewards of the public trust; we use intelligence authorities and resources prudently, protect intelligence sources and methods diligently, report wrongdoing through appropriate channels; and remain accountable to ourselves, our oversight institutions, and through those institutions, ultimately to the American people.

EXCELLENCE

We seek to improve our performance and our craft continuously, share information responsibly, collaborate with our colleagues, and demonstrate innovation and agility when meeting new challenges.

DIVERSITY

We embrace the diversity of our Nation, promote diversity and inclusion in our work force, and encourage diversity in our thinking.

**PRINCIPLES OF INTELLIGENCE TRANSPARENCY FOR THE
INTELLIGENCE COMMUNITY**

The *Principles of Intelligence Transparency for the Intelligence Community* are intended to facilitate IC decisions on making information publicly available in a manner that enhances public understanding of intelligence activities, while continuing to protect information when disclosure would harm national security.

These Principles do not modify or supersede applicable laws, executive orders, and directives, including Executive Order 13526, Classified National Security Information. Instead, they articulate the general norms that elements of the IC should follow in implementing those authorities and requirements.

The Intelligence Community will:

1. Provide appropriate transparency to enhance public understanding about:
 - a. the IC's mission and what the IC does to accomplish it (including its structure and effectiveness);
 - b. the laws, directives, authorities, and policies that govern the IC's activities; and
 - c. the compliance and oversight framework that ensures intelligence activities are conducted in accordance with applicable rules.

2. Be proactive and clear in making information publicly available through authorized channels, including taking affirmative steps to:
 - a. provide timely transparency on matters of public interest;
 - b. prepare information with sufficient clarity and context, so that it is readily understandable;
 - c. make information accessible to the public through a range of communications channels, such as those enabled by new technology;
 - d. engage with stakeholders to better explain information and to understand diverse perspectives; and
 - e. in appropriate circumstances, describe why information cannot be made public.

3. In protecting information about intelligence sources, methods, and activities from unauthorized disclosure, ensure that IC professionals consistently and diligently execute their responsibilities to:
 - a. classify only that information which, if disclosed without authorization, could be expected to cause identifiable or describable damage to the national security;

- b. never classify information to conceal violations of law, inefficiency, or administrative error, or to prevent embarrassment;
- c. distinguish, through portion marking and similar means, classified and unclassified information; and
- d. consider the public interest to the maximum extent feasible when making classification determinations, while continuing to protect information as necessary to maintain intelligence effectiveness, protect the safety of those who work for or with the IC, or otherwise protect national security.

4. Align IC roles, resources, processes, and policies to support robust implementation of these principles, consistent with applicable laws, executive orders, and directives.

NATIONAL SECURITY ACT OF 1947

[Public Law 235; 61 STAT. 496; July 26, 1947]

AN ACT To promote the national security by providing for a Secretary of Defense; for a National Military Establishment; for a Department of the Army, a Department of the Navy, and a Department of the Air Force; and for the coordination of the activities of the National Military Establishment with other departments and agencies of the Government concerned with the national security.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SHORT TITLE

That this Act may be cited as the “National Security Act of 1947”.

TABLE OF CONTENTS

- SEC. 2. Declaration of Policy.
- SEC. 3. Definitions.

TITLE I—COORDINATION FOR NATIONAL SECURITY

- SEC. 101. National Security Council.
- SEC. 101A. Joint Intelligence Community Council.
- SEC. 102. Director of National Intelligence.
- SEC. 102A. Responsibilities and authorities of the Director of National Intelligence.
- SEC. 103. Office of the Director of National Intelligence.
- SEC. 103A. Deputy Directors of National Intelligence.
- SEC. 103B. National Intelligence Council.
- SEC. 103C. General Counsel.
- SEC. 103D. Civil Liberties Protection Officer.
- SEC. 103E. Director of Science and Technology.
- SEC. 103F. Director of the National Counterintelligence and Security Center.
- SEC. 103G. Chief Information Officer.
- SEC. 103H. Inspector General of the Intelligence Community.
- SEC. 103I. Chief Financial Officer of the Intelligence Community.
- SEC. 103J. Functional Managers for the intelligence community [*sic*].

NATIONAL SECURITY ACT OF 1947

- SEC. 103K. Intelligence Community Chief Data Officer.
- SEC. 103L. Intelligence Community Innovation Unit.
- SEC. 104. Central Intelligence Agency.
- SEC. 104A. Director of the Central Intelligence Agency.
- SEC. 104B. Deputy Director of the Central Intelligence Agency.
- SEC. 105. Responsibilities of the Secretary of Defense pertaining to the National Intelligence Program.
- SEC. 105A. Assistance to United States law enforcement agencies.
- SEC. 105B. Disclosure of foreign intelligence acquired in criminal investigations; notice of criminal investigations of foreign intelligence sources.
- SEC. 105C. Prohibition on collection and maintenance of information of United States persons based on First Amendment-protected activities.
- SEC. 106. Appointment of officials responsible for intelligence-related activities.
- SEC. 106A. Director of the National Reconnaissance Office.
- SEC. 108. Annual National Security Strategy Report.
- SEC. 108A. National intelligence strategy.
- SEC. 108B. Annual reports on world-wide threats.
- SEC. 109. Software licensing.
- SEC. 110. National mission of National Geospatial-Intelligence Agency.
- SEC. 112. Restrictions on intelligence sharing with the United Nations.
- SEC. 113. Detail of intelligence community personnel—intelligence community assignment program.
- SEC. 113A. Non-reimbursable detail of other personnel.
- SEC. 113B. Special pay authority for science, technology, engineering, or mathematics positions and positions requiring banking or financial services expertise.
- SEC. 114. Annual report on hiring and retention of minority employees.
- SEC. 115. Limitation on establishment or operation of diplomatic intelligence support centers.
- SEC. 116. Travel on any common carrier for certain intelligence collection personnel.
- SEC. 117. POW/MIA analytic capability.
- SEC. 118. Annual report on financial intelligence on terrorist assets.
- SEC. 119. National Counterterrorism Center.
- SEC. 119A. National Counterproliferation and Biosecurity Center.
- SEC. 119B. National intelligence centers.
- SEC. 119C. Foreign Malign Influence Center.
- SEC. 120. Climate Security Advisory Council.

NATIONAL SECURITY ACT OF 1947

- SEC. 121. Counterintelligence and national security protections for intelligence community grant funding.
- SEC. 122. Office of engagement.

TITLE II—THE DEPARTMENT OF DEFENSE

- SEC. 201. Applicable Laws.
- SEC. 205. Department of the Army.
- SEC. 206. Department of the Navy.
- SEC. 207. Department of the Air Force.

TITLE III—MISCELLANEOUS

- SEC. 301. National Security Agency voluntary separation.
- SEC. 302. Authority of Federal Bureau of Investigation to award personal services contracts.
- SEC. 303. Advisory committees and personnel.
- SEC. 304. Requirements for certain employment activities by former intelligence officers and employees.
- SEC. 307. Authorization for appropriations.
- SEC. 308. Definitions.
- SEC. 309. Separability.
- SEC. 310. Effective date.
- SEC. 311. Succession to the Presidency.
- SEC. 312. Repealing and saving provisions.
- SEC. 313. Insider threat policy compliance and reporting.

TITLE V—ACCOUNTABILITY FOR INTELLIGENCE ACTIVITIES

- SEC. 501. General congressional oversight provisions.
- SEC. 501A. Congressional oversight of controlled access programs
- SEC. 502. Reporting of intelligence activities other than covert actions.
- SEC. 503. Presidential approval and reporting of covert actions.
- SEC. 504. Funding of intelligence activities.
- SEC. 505. Notice to Congress of certain transfers of defense articles and defense services.
- SEC. 506. Specificity of National Intelligence Program budget amounts for counterterrorism, counterproliferation, counternarcotics, and counterintelligence.

NATIONAL SECURITY ACT OF 1947

- SEC. 506A. Budget treatment of costs of acquisition of major systems by the intelligence community.
- SEC. 506B. Annual personnel level assessments for the intelligence community.
- SEC. 506C. Vulnerability assessments of major systems.
- SEC. 506D. Intelligence community business system transformation.
- SEC. 506E. Reports on the acquisition of major systems.
- SEC. 506F. Critical cost growth in major systems.
- SEC. 506G. Future budget projections.
- SEC. 506H. Reports on security clearances.
- SEC. 506I. Summary of intelligence relating to terrorist recidivism of detainees held at United States Naval Station, Guantanamo Bay, Cuba.
- SEC. 506J. Classified intelligence budget justification materials.
- SEC. 507. Dates for submittal of various annual and semiannual reports to the congressional intelligence committees.
- SEC. 508. Certification of compliance with oversight requirements.
- SEC. 509. Auditability of certain elements of the intelligence community.
- SEC. 510. Significant interpretations of law concerning intelligence activities.
- SEC. 511. Annual report on violations of law or executive order.
- SEC. 512. Briefings and notifications on counterintelligence activities of the Federal Bureau of Investigation.
- SEC 513. Annual reports on the domestic activities
- SEC. 514. Unfunded priorities of the intelligence community: annual report.
- SEC. 515. Submission of covered documents and classified annexes.
- SEC. 516. Submission of legislative proposals.

TITLE VI—PROTECTION OF CERTAIN NATIONAL SECURITY INFORMATION

- SEC. 601. Protection of identities of certain United States undercover intelligence officers, agents, informants, and sources.
- SEC. 602. Defenses and exceptions.
- SEC. 603. Extraterritorial jurisdiction.
- SEC. 604. Providing information to Congress.
- SEC. 605. Definitions.

TITLE VII—PROTECTION OF OPERATIONAL FILES

- SEC. 701. Operational files of the Central Intelligence Agency.
- SEC. 702. Operational files of the National Geospatial-Intelligence Agency.
- SEC. 703. Operational files of the National Reconnaissance Office.
- SEC. 704. Operational files of the National Security Agency.

NATIONAL SECURITY ACT OF 1947

- SEC. 705. Operational files of the Defense Intelligence Agency.
- SEC. 706. Protection of certain files of the Office of the Director of National Intelligence.

TITLE VIII—ACCESS TO CLASSIFIED INFORMATION

- SEC. 801. Procedures.
- SEC. 802. Requests by authorized investigative agencies.
- SEC. 803. Security Executive Agent.
- SEC. 804. Exceptions.
- SEC. 805. Definitions.

TITLE IX—APPLICATION OF SANCTIONS LAWS TO
INTELLIGENCE ACTIVITIES

- SEC. 901. Stay of sanctions.
- SEC. 902. Extension of stay.
- SEC. 903. Reports.
- SEC. 904. Laws subject to stay.

TITLE X—EDUCATION IN SUPPORT OF NATIONAL INTELLIGENCE

SUBTITLE A—SCIENCE AND TECHNOLOGY

- SEC. 1001. Scholarships and work-study for pursuit of graduate degrees in science and technology.
- SEC. 1002. Framework for cross-disciplinary education and training.

SUBTITLE B—FOREIGN LANGUAGES PROGRAM

- SEC. 1011. Program on advancement of foreign languages critical to the intelligence community.
- SEC. 1012. Education partnerships.
- SEC. 1013. Voluntary services.
- SEC. 1014. Regulations.
- SEC. 1015. Definitions.

SUBTITLE C—ADDITIONAL EDUCATION PROVISIONS

- SEC. 1021. Assignment of intelligence community personnel as language students.

NATIONAL SECURITY ACT OF 1947

- SEC. 1022. Program on recruitment and training.
- SEC. 1023. Educational scholarship program.
- SEC. 1024. Intelligence officer training program.
- SEC. 1025. Authorization of support by Director of National Intelligence for certain workforce activities.

SUBTITLE D—NATIONAL INTELLIGENCE UNIVERSITY

- SEC. 1031. Transfer date.
- SEC. 1032. Degree-granting authority.
- SEC. 1033. Reporting.
- SEC. 1034. Continued applicability of the Federal Advisory Committee Act to the Board of Visitors.

TITLE XI—OTHER PROVISIONS

- SEC. 1101. Applicability to United States intelligence activities of Federal laws implementing international treaties and agreements.
- SEC. 1102. Counterintelligence initiatives.
- SEC. 1102A. Measures to mitigate counterintelligence threats from proliferation and use of foreign commercial spyware.
- SEC. 1103. Misuse of the Office of the Director of National Intelligence name, initials, or seal.
- SEC. 1104. Prohibited personnel practices in the Intelligence Community.
- SEC. 1105. Semiannual reports on investigations of unauthorized disclosures of classified information.
- SEC. 1105A. Notice and damage assessment with respect to significant unauthorized disclosure or compromise of classified national intelligence.
- SEC. 1106. Inspector General external review panel.
- SEC. 1107. Annual reports on influence operations and campaigns in the United States by the Chinese Communist Party.
- SEC. 1107A. Annual reports on security services of the People's Republic of China in the Hong Kong Special Administration Region.
- SEC. 1108. Annual reports on influence operations and campaigns in the United States by the Russian Federation.
- SEC. 1109. Requirement to buy certain satellite component from American sources.
- SEC. 1110. Report on best practices to protect privacy, civil liberties, and civil rights of Chinese Americans.
- SEC. 1111. Biennial reports on foreign biological threats.

NATIONAL SECURITY ACT OF 1947

- SEC. 1112. Annual reports on certain cyber vulnerabilities procured by intelligence community and foreign commercial providers of cyber vulnerabilities.
- SEC. 1113. Periodic reports on technology strategy of intelligence community.
- SEC. 1114. Annual report on reporting requirements.

DECLARATION OF POLICY

SEC. 2. [50 U.S.C. § 3002]

In enacting this legislation, it is the intent of Congress to provide a comprehensive program for the future security of the United States; to provide for the establishment of integrated policies and procedures for the departments, agencies, and functions of the Government relating to the national security; to provide a Department of Defense, including the three military Departments of the Army, the Navy (including naval aviation and the United States Marine Corps), and the Air Force under the direction, authority, and control of the Secretary of Defense; to provide that each military department shall be separately organized under its own Secretary and shall function under the direction, authority, and control of the Secretary of Defense; to provide for their unified direction under civilian control of the Secretary of Defense but not to merge these departments or services; to provide for the establishment of unified or specified combatant commands, and a clear and direct line of command to such commands; to eliminate unnecessary duplication in the Department of Defense, and particularly in the field of research and engineering by vesting its overall direction and control in the Secretary of Defense; to provide more effective, efficient, and economical administration in the Department of Defense; to provide for the unified strategic direction of the combatant forces, or their operation under unified command, and for their integration into an efficient team of land, naval, and air forces but not to establish a single Chief of Staff over the armed forces nor an overall armed forces general staff.

DEFINITIONS

SEC. 3. [50 U.S.C. § 3003]

As used in this Act:

- (1) The term “intelligence” includes foreign intelligence and counterintelligence.
- (2) The term “foreign intelligence” means information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities.
- (3) The term “counterintelligence” means information gathered, and activities conducted, to protect against espionage, other intelligence activities, sabotage, or

NATIONAL SECURITY ACT OF 1947

assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities.

- (4) The term “intelligence community” includes the following:
- (A) The Office of the Director of National Intelligence.
 - (B) The Central Intelligence Agency.
 - (C) The National Security Agency.
 - (D) The Defense Intelligence Agency.
 - (E) The National Geospatial-Intelligence Agency.
 - (F) The National Reconnaissance Office.
 - (G) Other offices within the Department of Defense for the collection of specialized national intelligence through reconnaissance programs.
 - (H) The intelligence elements of the Army, the Navy, the Air Force, the Marine Corps, the Space Force, the Coast Guard, the Federal Bureau of Investigation, the Drug Enforcement Administration, and the Department of Energy.
 - (I) The Bureau of Intelligence and Research of the Department of State.
 - (J) The Office of Intelligence and Analysis of the Department of the Treasury.
 - (K) The Office of Intelligence and Analysis of the Department of Homeland Security.
 - (L) Such other elements of any department or agency as may be designated by the President, or designated jointly by the Director of National Intelligence and the head of the department or agency concerned, as an element of the intelligence community.
- (5) The terms “national intelligence” and “intelligence related to national security” refer to all intelligence, regardless of the source from which derived and including information gathered within or outside the United States, that—
- (A) pertains, as determined consistent with any guidance issued by the President, to more than one United States Government agency; and
 - (B) that involves—
 - (i) threats to the United States, its people, property, or interests;
 - (ii) the development, proliferation, or use of weapons of mass destruction; or
 - (iii) any other matter bearing on United States national or homeland security.
- (6) The term “National Intelligence Program” refers to all programs, projects, and activities of the intelligence community, as well as any other programs of the intelligence community designated jointly by the Director of National Intelligence and the head of a United States department or agency or by the President. Such term does not include programs, projects, or activities of the

military departments to acquire intelligence solely for the planning and conduct of tactical military operations by United States Armed Forces.

(7) The term “congressional intelligence committees” means—

(A) the Select Committee on Intelligence of the Senate; and

(B) the Permanent Select Committee on Intelligence of the House of Representatives.

TITLE I—COORDINATION FOR NATIONAL SECURITY

NATIONAL SECURITY COUNCIL

SEC. 101. [50 U.S.C. § 3021]

(a) NATIONAL SECURITY COUNCIL.—There is a council known as the National Security Council (in this section referred to as the “Council”).

(b) FUNCTIONS.—Consistent with the direction of the President, the functions of the Council shall be to—

(1) advise the President with respect to the integration of domestic, foreign, and military policies relating to the national security so as to enable the Armed Forces and the other departments and agencies of the United States Government to cooperate more effectively in matters involving the national security;

(2) assess and appraise the objectives, commitments, and risks of the United States in relation to the actual and potential military power of the United States, and make recommendations thereon to the President;

(3) make recommendations to the President concerning policies on matters of common interest to the departments and agencies of the United States Government concerned with the national security; and

(4) coordinate, without assuming operational authority, the United States Government response to malign foreign influence operations and campaigns.

(c) MEMBERSHIP.—

(1) IN GENERAL.—The Council consists of the President, the Vice President, the Secretary of State, the Secretary of Defense, the Secretary of Energy, the Secretary of the Treasury, the Director of the Office of Pandemic Preparedness and Response Policy, and such other officers of the United States Government as the President may designate.

(2) ATTENDANCE AND PARTICIPATION IN MEETINGS.—The President may designate such other officers of the United States Government as the President considers appropriate, including the Director of National Intelligence, the Director of National Drug Control Policy, and the Chairman of the Joint Chiefs of Staff, and the National Cyber Director, to attend and participate in meetings of the Council.

NATIONAL SECURITY ACT OF 1947

(d) **PRESIDING OFFICERS.**—At meetings of the Council, the President shall preside or, in the absence of the President, a member of the Council designated by the President shall preside.

(e) **STAFF.**—

(1) **IN GENERAL.**—The Council shall have a staff headed by a civilian executive secretary appointed by the President.

(2) **STAFF.**—Consistent with the direction of the President and subject to paragraph (3), the executive secretary may, subject to the civil service laws and chapter 51 and subchapter III of chapter 53 of title 5, United States Code, appoint and fix the compensation of such personnel as may be necessary to perform such duties as may be prescribed by the President in connection with performance of the functions of the Council.

(3) **NUMBER OF PROFESSIONAL STAFF.**—The professional staff for which this subsection provides shall not exceed 200 persons, including persons employed by, assigned to, detailed to, under contract to serve on, or otherwise serving or affiliated with the staff. The limitation in this paragraph does not apply to personnel serving substantially in support or administrative positions.

(f) **SPECIAL ADVISOR TO THE PRESIDENT ON INTERNATIONAL RELIGIOUS FREEDOM.**—It is the sense of Congress that there should be within the staff of the Council a Special Adviser to the President on International Religious Freedom, whose position should be comparable to that of a director within the Executive Office of the President. The Special Adviser should serve as a resource for executive branch officials, compiling and maintaining information on the facts and circumstances of violations of religious freedom (as defined in section 3 of the International Religious Freedom Act of 1998 (22 U.S.C. 6402)), and making policy recommendations. The Special Adviser should serve as liaison with the Ambassador at Large for International Religious Freedom, the United States Commission on International Religious Freedom, Congress and, as advisable, religious nongovernmental organizations.

(g) **COORDINATOR FOR COMBATING MALIGN FOREIGN INFLUENCE OPERATIONS AND CAMPAIGNS.**—

(1) **IN GENERAL.**—The President shall designate an employee of the National Security Council to be responsible for the coordination of the interagency process for combating malign foreign influence operations and campaigns.

(2) **CONGRESSIONAL BRIEFING.**—

(A) **IN GENERAL.**—Not less frequently than twice each year, the employee designated under this subsection, or the employee's designee, shall provide to the congressional committees specified

in subparagraph (B) a briefing on the responsibilities and activities of the employee designated under this subsection.

(B) COMMITTEES SPECIFIED.—The congressional committees specified in this subparagraph are the following:

(i) The Committees on Armed Services, Foreign Affairs, and Oversight and Government Reform, and the Permanent Select Committee on Intelligence of the House of Representatives.

(ii) The Committees on Armed Services, Foreign Relations, and Homeland Security and Governmental Affairs, and the Select Committee on Intelligence of the Senate.

(h) DEFINITION OF MALIGN FOREIGN INFLUENCE OPERATIONS AND CAMPAIGNS.—In this section, the term “malign foreign influence operations and campaigns” means the coordinated, direct or indirect application of national diplomatic, informational, military, economic, business, corruption, educational, and other capabilities by hostile foreign powers to affect attitudes, behaviors, decisions, or outcomes within the United States.

JOINT INTELLIGENCE COMMUNITY COUNCIL

SEC. 101A. [50 U.S.C. § 3022]

(a) JOINT INTELLIGENCE COMMUNITY COUNCIL.—There is a Joint Intelligence Community Council.

(b) MEMBERSHIP.—The Joint Intelligence Community Council shall consist of the following:

(1) The Director of National Intelligence, who shall chair the Council.

(2) The Secretary of State.

(3) The Secretary of the Treasury.

(4) The Secretary of Defense.

(5) The Attorney General.

(6) The Secretary of Energy.

(7) The Secretary of Homeland Security.

(8) Such other officers of the United States Government as the President may designate from time to time.

(c) FUNCTIONS.—The Joint Intelligence Community Council shall assist the Director of National Intelligence in developing and implementing a joint, unified national intelligence effort to protect national security by—

(1) advising the Director on establishing requirements, developing budgets, financial management, and monitoring and evaluating the performance of the intelligence community, and on such other matters as the Director may request; and

NATIONAL SECURITY ACT OF 1947

(2) ensuring the timely execution of programs, policies, and directives established or developed by the Director.

(d) MEETINGS.—The Director of National Intelligence shall convene meetings of the Joint Intelligence Community Council as the Director considers appropriate.

(e) ADVICE AND OPINIONS OF MEMBERS OTHER THAN CHAIRMAN.—

(1) A member of the Joint Intelligence Community Council (other than the Chairman) may submit to the Chairman advice or an opinion in disagreement with, or advice or an opinion in addition to, the advice presented by the Director of National Intelligence to the President or the National Security Council, in the role of the Chairman as Chairman of the Joint Intelligence Community Council. If a member submits such advice or opinion, the Chairman shall present the advice or opinion of such member at the same time the Chairman presents the advice of the Chairman to the President or the National Security Council, as the case may be.

(2) The Chairman shall establish procedures to ensure that the presentation of the advice of the Chairman to the President or the National Security Council is not unduly delayed by reason of the submission of the individual advice or opinion of another member of the Council.

(f) RECOMMENDATIONS TO CONGRESS.—Any member of the Joint Intelligence Community Council may make such recommendations to Congress relating to the intelligence community as such member considers appropriate.

DIRECTOR OF NATIONAL INTELLIGENCE

SEC. 102. [50 U.S.C. § 3023]

(a) DIRECTOR OF NATIONAL INTELLIGENCE.—

(1) There is a Director of National Intelligence who shall be appointed by the President, by and with the advice and consent of the Senate. Any individual nominated for appointment as Director of National Intelligence shall have extensive national security expertise.

(2) The Director of National Intelligence shall not be located within the Executive Office of the President.

(b) PRINCIPAL RESPONSIBILITY.—Subject to the authority, direction, and control of the President, the Director of National Intelligence shall—

(1) serve as head of the intelligence community;

(2) act as the principal adviser to the President, to the National Security Council, and the Homeland Security Council for intelligence matters related to the national security; and

(3) consistent with section 1018 of the National Security Intelligence Reform Act of 2004, oversee and direct the implementation of the National Intelligence Program.

(c) **PROHIBITION ON DUAL SERVICE.**—The individual serving in the position of Director of National Intelligence shall not, while so serving, also serve as the Director of the Central Intelligence Agency or as the head of any other element of the intelligence community.

**RESPONSIBILITIES AND AUTHORITIES OF
THE DIRECTOR OF NATIONAL INTELLIGENCE**

SEC. 102A. [50 U.S.C. § 3024]

(a) **PROVISION OF INTELLIGENCE.**—

(1) The Director of National Intelligence shall be responsible for ensuring that national intelligence is provided—

(A) to the President;

(B) to the heads of departments and agencies of the executive branch;

(C) to the Chairman of the Joint Chiefs of Staff and senior military commanders;

(D) to the Senate and House of Representatives and the committees thereof; and

(E) to such other persons as the Director of National Intelligence determines to be appropriate.

(2) Such national intelligence should be timely, objective, independent of political considerations, and based upon all sources available to the intelligence community and other appropriate entities.

(b) **ACCESS TO INTELLIGENCE.**—Unless otherwise directed by the President, the Director of National Intelligence shall have access to all national intelligence and intelligence related to the national security which is collected by any Federal department, agency, or other entity, except as otherwise provided by law or, as appropriate, under guidelines agreed upon by the Attorney General and the Director of National Intelligence.

(c) **BUDGET AUTHORITIES.**—

(1) With respect to budget requests and appropriations for the National Intelligence Program, the Director of National Intelligence shall—

(A) based on intelligence priorities set by the President, provide to the heads of departments containing agencies or organizations within the intelligence community, and to the heads of such agencies and organizations, guidance for developing the National Intelligence Program budget pertaining to such agencies and organizations;

(B) based on budget proposals provided to the Director of National Intelligence by the heads of agencies and organizations within the intelligence community and the heads of their respective departments and, as appropriate, after obtaining the advice of the Joint Intelligence Community Council, develop and determine an annual consolidated National Intelligence Program budget; and

(C) present such consolidated National Intelligence Program budget, together with any comments from the heads of departments containing agencies or organizations within the intelligence community, to the President for approval.

(2) In addition to the information provided under paragraph (1)(B), the heads of agencies and organizations within the intelligence community shall provide the Director of National Intelligence such other information as the Director shall request for the purpose of determining the annual consolidated National Intelligence Program budget under that paragraph.

(3)(A) The Director of National Intelligence shall participate in the development by the Secretary of Defense of the annual budget for the Military Intelligence Program or any successor program or programs.

(B) The Director of National Intelligence shall provide guidance for the development of the annual budget for each element of the intelligence community that is not within the National Intelligence Program.

(4) The Director of National Intelligence shall ensure the effective execution of the annual budget for intelligence and intelligence-related activities.

(5)(A) The Director of National Intelligence shall be responsible for managing appropriations for the National Intelligence Program by directing the allotment or allocation of such appropriations through the heads of the departments containing agencies or organizations within the intelligence community and the Director of the Central Intelligence Agency, with prior notice (including the provision of appropriate supporting information) to the head of the department containing an agency or organization receiving any such allocation or allotment or the Director of the Central Intelligence Agency.

(B) Notwithstanding any other provision of law, pursuant to relevant appropriations Acts for the National Intelligence Program, the Director of the Office of Management and Budget shall exercise the authority of the Director of the Office of Management and Budget to apportion funds, at the exclusive direction of the Director of National Intelligence, for allocation to the elements of the intelligence community through the

relevant host executive departments and the Central Intelligence Agency. Department comptrollers or appropriate budget execution officers shall allot, allocate, reprogram, or transfer funds appropriated for the National Intelligence Program in an expeditious manner.

(C) The Director of National Intelligence shall monitor the implementation and execution of the National Intelligence Program by the heads of the elements of the intelligence community that manage programs and activities that are part of the National Intelligence Program, which shall include audits and evaluations.

(D) Consistent with subparagraph (C), the Director of National Intelligence shall ensure that the programs and activities that are part of the National Intelligence Program, including those of the Federal Bureau of Investigation, are structured and executed in a manner that enables budget traceability.

(6) Apportionment and allotment of funds under this subsection shall be subject to chapter 13 and section 1517 of title 31, United States Code, and the Congressional Budget and Impoundment Control Act of 1974 (2 U.S.C. 621 et seq.).

(7)(A) The Director of National Intelligence shall provide a semi-annual report, beginning April 1, 2005, and ending April 1, 2007, to the President and the Congress regarding implementation of this section.

(B) The Director of National Intelligence shall report to the President and the Congress not later than 15 days after learning of any instance in which a departmental comptroller acts in a manner inconsistent with the law (including permanent statutes, authorization Acts, and appropriations Acts), or the direction of the Director of National Intelligence, in carrying out the National Intelligence Program.

(d) ROLE OF DIRECTOR OF NATIONAL INTELLIGENCE IN TRANSFER AND REPROGRAMMING OF FUNDS.—

(1)(A) No funds made available under the National Intelligence Program may be transferred or reprogrammed without the prior approval of the Director of National Intelligence, except in accordance with procedures prescribed by the Director of National Intelligence.

(B) The Secretary of Defense shall consult with the Director of National Intelligence before transferring or reprogramming funds made available under the Military Intelligence Program or any successor program or programs.

- (2) Subject to the succeeding provisions of this subsection, the Director of National Intelligence may transfer or reprogram funds appropriated for a program within the National Intelligence Program—
- (A) to another such program;
 - (B) to other departments or agencies of the United States Government for the development and fielding of systems of common concern related to the collection, processing, analysis, exploitation, and dissemination of intelligence information; or
 - (C) to a program funded by appropriations not within the National Intelligence Program to address critical gaps in intelligence information sharing or access capabilities.
- (3) The Director of National Intelligence may only transfer or reprogram funds referred to in paragraph (1)(A)—
- (A) with the approval of the Director of the Office of Management and Budget; and
 - (B) after consultation with the heads of departments containing agencies or organizations within the intelligence community to the extent such agencies or organizations are affected, and, in the case of the Central Intelligence Agency, after consultation with the Director of the Central Intelligence Agency.
- (4) The amounts available for transfer or reprogramming in the National Intelligence Program in any given fiscal year, and the terms and conditions governing such transfers and reprogrammings, are subject to the provisions of annual appropriations Acts and this subsection.
- (5)(A) A transfer or reprogramming of funds may be made under this subsection only if—
- (i) the funds are being transferred to an activity that is a higher priority intelligence activity;
 - (ii) the transfer or reprogramming supports an emergent need, improves program effectiveness, or increases efficiency;
 - (iii) the transfer or reprogramming does not involve a transfer or reprogramming of funds to a Reserve for Contingencies of the Director of National Intelligence or the Reserve for Contingencies of the Central Intelligence Agency;
 - (iv) the transfer or reprogramming results in a cumulative transfer or reprogramming of funds out of any department or agency, as appropriate, funded in the National Intelligence Program in a single fiscal year—
 - (I) that is less than \$150,000,000, and

(II) that is less than 5 percent of amounts available to a department or agency under the National Intelligence Program; and

(v) the transfer or reprogramming does not terminate an acquisition program.

(B) A transfer or reprogramming may be made without regard to a limitation set forth in clause (iv) or (v) of subparagraph (A) if the transfer has the concurrence of the head of the department involved or the Director of the Central Intelligence Agency (in the case of the Central Intelligence Agency). The authority to provide such concurrence may only be delegated by the head of the department involved or the Director of the Central Intelligence Agency (in the case of the Central Intelligence Agency) to the deputy of such officer.

(6) Funds transferred or reprogrammed under this subsection shall remain available for the same period as the appropriations account to which transferred or reprogrammed.

(7) Any transfer or reprogramming of funds under this subsection shall be carried out in accordance with existing procedures applicable to reprogramming notifications for the appropriate congressional committees. Any proposed transfer or reprogramming for which notice is given to the appropriate congressional committees shall be accompanied by a report explaining the nature of the proposed transfer or reprogramming and how it satisfies the requirements of this subsection. In addition, the congressional intelligence committees shall be promptly notified of any transfer or reprogramming of funds made pursuant to this subsection in any case in which the transfer or reprogramming would not have otherwise required reprogramming notification under procedures in effect as of the date of the enactment of this subsection.

(e) TRANSFER OF PERSONNEL.—

(1)(A) In addition to any other authorities available under law for such purposes, in the first twelve months after establishment of a new national intelligence center, the Director of National Intelligence, with the approval of the Director of the Office of Management and Budget and in consultation with the congressional committees of jurisdiction referred to in subparagraph (B), may transfer not more than 100 personnel authorized for elements of the intelligence community to such center.

(B) The Director of National Intelligence shall promptly provide notice of any transfer of personnel made pursuant to this paragraph to—

(i) the congressional intelligence committees;

- (ii) the Committees on Appropriations of the Senate and the House of Representatives;
- (iii) in the case of the transfer of personnel to or from the Department of Defense, the Committees on Armed Services of the Senate and the House of Representatives; and
- (iv) in the case of the transfer of personnel to or from the Department of Justice, to the Committees on the Judiciary of the Senate and the House of Representatives.

(C) The Director shall include in any notice under subparagraph (B) an explanation of the nature of the transfer and how it satisfies the requirements of this subsection.

(2)(A) The Director of National Intelligence, with the approval of the Director of the Office of Management and Budget and in accordance with procedures to be developed by the Director of National Intelligence and the heads of the departments and agencies concerned, may transfer personnel authorized for an element of the intelligence community to another such element for a period of not more than 2 years.

(B) A transfer of personnel may be made under this paragraph only if—

- (i) the personnel are being transferred to an activity that is a higher priority intelligence activity; and
- (ii) the transfer supports an emergent need, improves program effectiveness, or increases efficiency.

(C) The Director of National Intelligence shall promptly provide notice of any transfer of personnel made pursuant to this paragraph to—

- (i) the congressional intelligence committees;
- (ii) in the case of the transfer of personnel to or from the Department of Defense, the Committees on Armed Services of the Senate and the House of Representatives; and
- (iii) in the case of the transfer of personnel to or from the Department of Justice, to the Committees on the Judiciary of the Senate and the House of Representatives.

(D) The Director shall include in any notice under subparagraph (C) an explanation of the nature of the transfer and how it satisfies the requirements of this paragraph.

(3)(A) In addition to the number of full-time equivalent positions authorized for the Office of the Director of National Intelligence for a fiscal year, there is authorized for such Office for each fiscal year an additional 100 full-time equivalent positions that may be used only for the purposes described in subparagraph (B).

(B) Except as provided in subparagraph (C), the Director of National Intelligence may use a full-time equivalent position authorized under subparagraph (A) only for the purpose of providing a temporary transfer of personnel made in accordance with paragraph (2) to an element of the intelligence community to enable such element to increase the total number of personnel authorized for such element, on a temporary basis—

(i) during a period in which a permanent employee of such element is absent to participate in critical language training; or

(ii) to accept a permanent employee of another element of the intelligence community to provide language-capable services.

(C) Paragraph (2)(B) shall not apply with respect to a transfer of personnel made under subparagraph (B).

(D) For each of the fiscal years 2010, 2011, and 2012, the Director of National Intelligence shall submit to the congressional intelligence committees an annual report on the use of authorities under this paragraph. Each such report shall include a description of—

(i) the number of transfers of personnel made by the Director pursuant to subparagraph (B), disaggregated by each element of the intelligence community;

(ii) the critical language needs that were fulfilled or partially fulfilled through the use of such transfers; and

(iii) the cost to carry out subparagraph (B).

(4) It is the sense of Congress that—

(A) the nature of the national security threats facing the United States will continue to challenge the intelligence community to respond rapidly and flexibly to bring analytic resources to bear against emerging and unforeseen requirements;

(B) both the Office of the Director of National Intelligence and any analytic centers determined to be necessary should be fully and properly supported with appropriate levels of personnel resources and that the President's yearly budget requests adequately support those needs; and

(C) the President should utilize all legal and administrative discretion to ensure that the Director of National Intelligence and all other elements of the intelligence community have the necessary resources and procedures to respond promptly and effectively to emerging and unforeseen national security challenges.

(f) TASKING AND OTHER AUTHORITIES.—

(1)(A) The Director of National Intelligence shall—

(i) establish objectives, priorities, and guidance for the intelligence community to ensure timely and effective collection, processing, analysis, and dissemination (including access by users to collected data consistent with applicable law and, as appropriate, the guidelines referred to in subsection (b) and analytic products generated by or within the intelligence community) of national intelligence;

(ii) determine requirements and priorities for, and manage and direct the tasking of, collection, analysis, production, and dissemination of national intelligence by elements of the intelligence community, including—

(I) approving requirements (including those requirements responding to needs provided by consumers) for collection and analysis; and

(II) resolving conflicts in collection requirements and in the tasking of national collection assets of the elements of the intelligence community; and

(iii) provide advisory tasking to intelligence elements of those agencies and departments not within the National Intelligence Program.

(B) The authority of the Director of National Intelligence under subparagraph (A) shall not apply—

(i) insofar as the President so directs;

(ii) with respect to clause (ii) of subparagraph (A), insofar as the Secretary of Defense exercises tasking authority under plans or arrangements agreed upon by the Secretary of Defense and the Director of National Intelligence; or

(iii) to the direct dissemination of information to State government and local government officials and private sector entities pursuant to sections 201 and 892 of the Homeland Security Act of 2002 (6 U.S.C. 121, 482).

(2) The Director of National Intelligence shall oversee the National Counterterrorism Center, the National Counterproliferation [and Biosecurity] Center, and the National Counterintelligence and Security Center and may establish such other national intelligence centers as the Director determines necessary.

(3)(A) The Director of National Intelligence shall prescribe, in consultation with the heads of other agencies or elements of the intelligence community, and the heads of their respective departments, binding personnel policies and programs applicable to the intelligence community that—

(i) require and facilitate assignments and details of personnel to national intelligence centers, and between elements of the intelligence community over the course of the careers of such personnel;

(ii) set standards for education, training, and career development of personnel of the intelligence community;

(iii) encourage and facilitate the recruitment and retention by the intelligence community of highly qualified individuals for the effective conduct of intelligence activities;

(iv) ensure that the personnel of the intelligence community are sufficiently diverse for purposes of the collection and analysis of intelligence through the recruitment and training of women, minorities, and individuals with diverse ethnic, cultural, and linguistic backgrounds;

(v) require service in more than one element of the intelligence community as a condition of promotion to such positions within the intelligence community as the Director shall specify, and take requisite steps to ensure compliance among elements of the intelligence community; and

(vi) ensure the effective management of intelligence community personnel who are responsible for intelligence community-wide matters.

(B) Policies prescribed under subparagraph (A) shall not be inconsistent with the personnel policies otherwise applicable to members of the uniformed services.

(4) The Director of National Intelligence shall ensure compliance with the Constitution and laws of the United States by the Central Intelligence Agency and shall ensure such compliance by other elements of the

intelligence community through the host executive departments that manage the programs and activities that are part of the National Intelligence Program.

(5) The Director of National Intelligence shall ensure the elimination of waste and unnecessary duplication within the intelligence community.

(6) The Director of National Intelligence shall establish requirements and priorities for foreign intelligence information to be collected under the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.), and provide assistance to the Attorney General to ensure that information derived from electronic surveillance or physical searches under that Act is disseminated so it may be used efficiently and effectively for national intelligence purposes, except that the Director shall have no authority to direct or undertake electronic surveillance or physical search operations pursuant to that Act unless authorized by statute or Executive order.

(7)(A) The Director of National Intelligence shall, if the Director determines it is necessary, or may, if requested by a congressional intelligence committee, conduct an accountability review of an element of the intelligence community or the personnel of such element in relation to a failure or deficiency within the intelligence community.

(B) The Director of National Intelligence, in consultation with the Attorney General, shall establish guidelines and procedures for conducting an accountability review under subparagraph (A).

(C)(i) The Director of National Intelligence shall provide the findings of an accountability review conducted under subparagraph (A) and the Director's recommendations for corrective or punitive action, if any, to the head of the applicable element of the intelligence community. Such recommendations may include a recommendation for dismissal of personnel.

(ii) If the head of such element does not implement a recommendation made by the Director under clause (i), the head of such element shall submit to the congressional intelligence committees a notice of the determination not to implement the recommendation, including the reasons for the determination.

(D) The requirements of this paragraph shall not be construed to limit any authority of the Director of National Intelligence under subsection (m) or with respect to supervision of the Central Intelligence Agency.

(8) The Director of National Intelligence shall—

(A) conduct assessments and audits of the compliance of each element of the intelligence community with minimum

insider threat policy;

(B) receive information from each element of the intelligence community regarding the collection, sharing, and use by such element of audit and monitoring data for insider threat detection across all classified and unclassified information technology systems within such element;

(C) provide guidance and oversight to Federal departments and agencies to fully implement automated records checks, consistent with personnel vetting reforms and the Trusted Workforce 2.0 initiative, or successor initiative, and ensure that information collected pursuant to such records checks is appropriately shared in support of intelligence community-wide insider threat initiatives;

(D) carry out evaluations of the effectiveness of counterintelligence, security, and insider threat program activities of each element of the intelligence community, including with respect to the lowest organizational unit of each such element, that include an identification of any gaps, shortfalls, or resource needs of each such element;

(E) identify gaps, shortfalls, resources needs, and recommendations for adjustments in allocations and additional resources and other remedies to strengthen counterintelligence, security, and insider threat detection programs;

(F) pursuant to final damage assessments facilitated by the National Counterintelligence and Security Center that have been undertaken as a result of an unauthorized disclosure, determine whether the heads of the elements of the intelligence community implement recommended mitigation, and notify the congressional intelligence committees of such determinations and notify the Committee on Armed Services of the Senate and the Committee on Armed Services of the House of Representatives in cases involving elements of the intelligence community within the Department of Defense; and

(G) study the data collected during the course of background investigations and adjudications for security clearances granted to individuals who subsequently commit unauthorized disclosures, and issue findings regarding the quality of such data as a predictor for insider threat activity, delineated by the severity of the unauthorized disclosure.

(9) The Director of National Intelligence shall ensure there is established a policy for minimum insider threat standards for the intelligence

community and ensure compliance by the elements of the intelligence community with that policy.

(10) The Director of National Intelligence shall perform such other intelligence-related functions as the President may direct.

(11) Nothing in this title shall be construed as affecting the role of the Department of Justice or the Attorney General under the Foreign Intelligence Surveillance Act of 1978.

(g) INTELLIGENCE INFORMATION SHARING.—

(1) The Director of National Intelligence shall have principal authority to ensure maximum availability of and access to intelligence information within the intelligence community consistent with national security requirements. The Director of National Intelligence shall—

(A) establish uniform security standards and procedures;

(B) establish common information technology standards, protocols, and interfaces;

(C) ensure development of information technology systems that include multi-level security and intelligence integration capabilities;

(D) establish policies and procedures to resolve conflicts between the need to share intelligence information and the need to protect intelligence sources and methods;

(E) develop an enterprise architecture for the intelligence community and ensure that elements of the intelligence community comply with such architecture;

(F) have procurement approval authority over all enterprise architecture-related information technology items funded in the National Intelligence Program; and

(G) in accordance with Executive Order No. 13526 (75 Fed. Reg. 707; relating to classified national security information) (or any subsequent corresponding executive order), and part 2001 of title 32, Code of Federal Regulations (or any subsequent corresponding regulation), establish—

(i) guidance to standardize, in appropriate cases, the formats for classified and unclassified intelligence products created by elements of the intelligence community for purposes of promoting the sharing of intelligence products; and

(ii) policies and procedures requiring the increased use, in appropriate cases, and including portion markings, of the classification of portions of information within one intelligence product.

(2) The President shall ensure that the Director of National Intelligence has all necessary support and authorities to fully and effectively implement paragraph (1).

(3) Except as otherwise directed by the President or with the specific written agreement of the head of the department or agency in question, a Federal agency or official shall not be considered to have met any obligation to provide any information, report, assessment, or other material (including unevaluated intelligence information) to that department or agency solely by virtue of having provided that information, report, assessment, or other material to the Director of National Intelligence or the National Counterterrorism Center.

(4) The Director of National Intelligence shall, in a timely manner, report to Congress any statute, regulation, policy, or practice that the Director believes impedes the ability of the Director to fully and effectively ensure maximum availability of access to intelligence information within the intelligence community consistent with the protection of the national security of the United States.

(h) ANALYSIS.—To ensure the most accurate analysis of intelligence is derived from all sources to support national security needs, the Director of National Intelligence shall—

(1) implement policies and procedures—

(A) to require sound analytic methods and tradecraft, independent of political considerations, throughout the elements of the intelligence community;

(B) to ensure that analysis is based upon all sources available; and

(C) to ensure that the elements of the intelligence community regularly conduct competitive analysis of analytic products, whether such products are produced by or disseminated to such elements;

(2) ensure that resource allocation for intelligence analysis is appropriately proportional to resource allocation for intelligence collection systems and operations in order to maximize analysis of all collected data;

(3) ensure that substantial differences in analytic judgment are fully considered, brought to the attention of policymakers, and documented in analytic products; and

(4) ensure that sufficient relationships are established between intelligence collectors and analysts to facilitate greater understanding of the needs of analysts.

(i) PROTECTION OF INTELLIGENCE SOURCES AND METHODS.—

(1) The Director of National Intelligence shall protect, and shall establish and enforce policies to protect, intelligence sources and methods from unauthorized disclosure.

(2) Consistent with paragraph (1), in order to maximize the dissemination of intelligence, the Director of National Intelligence shall establish and implement requirements for the intelligence community for the following purposes:

(A) Classification of information under applicable law, Executive orders, or other Presidential directives.

(B) Access to and dissemination of intelligence, both in final form and in the form when initially gathered.

(C) Preparation of intelligence products in such a way that source information is removed to allow for dissemination at the lowest level of classification possible or in unclassified form to the extent practicable.

(3) The Director may only delegate a duty or authority given the Director under this subsection to the Principal Deputy Director of National Intelligence.

(4)(A) Each head of an element of the intelligence community shall ensure that any congressionally mandated report submitted to Congress by the head, other than such a report submitted solely to the congressional intelligence committees, shall be consistent with the protection of intelligence sources and methods in accordance with the policies established by the Director under paragraph (1), regardless of whether the provision of law mandating the report explicitly requires such protection.

(B) Nothing in this paragraph shall be construed to alter any congressional leadership's or congressional committee's jurisdiction or access to information from any element of the intelligence community under the rules of either chamber of Congress.

(j) UNIFORM PROCEDURES FOR CLASSIFIED INFORMATION.—The Director of National Intelligence, subject to the direction of the President, shall—

(1) establish uniform standards and procedures for the grant of access to sensitive compartmented information to any officer or employee of any agency or department of the United States and to employees of contractors of those agencies or departments;

(2) ensure the consistent implementation of those standards and procedures throughout such agencies and departments;

- (3) ensure that security clearances granted by individual elements of the intelligence community are recognized by all elements of the intelligence community, and under contracts entered into by those agencies;
- (4) ensure that the process for investigation and adjudication of an application for access to sensitive compartmented information is performed in the most expeditious manner possible consistent with applicable standards for national security;
- (5) ensure that the background of each employee or officer of an element of the intelligence community, each contractor to an element of the intelligence community, and each individual employee of such a contractor who has been determined to be eligible for access to classified information is monitored on a continual basis under standards developed by the Director, including with respect to the frequency of evaluation, during the period of eligibility of such employee or officer of an element of the intelligence community, such contractor, or such individual employee to such a contractor to determine whether such employee or officer of an element of the intelligence community, such contractor, and such individual employee of such a contractor continues to meet the requirements for eligibility for access to classified information; and
- (6) develop procedures to require information sharing between elements of the intelligence community concerning potentially derogatory security information regarding an employee or officer of an element of the intelligence community, a contractor to an element of the intelligence community, or an individual employee of such a contractor that may impact the eligibility of such employee or officer of an element of the intelligence community, such contractor, or such individual employee of such a contractor for a security clearance.

(k) COORDINATION WITH FOREIGN GOVERNMENTS.—Under the direction of the President and in a manner consistent with section 207 of the Foreign Service Act of 1980 (22 U.S.C. 3927), the Director of National Intelligence shall oversee the coordination of the relationships between elements of the intelligence community and the intelligence or security services of foreign governments or international organizations on all matters involving intelligence related to the national security or involving intelligence acquired through clandestine means.

(l) ENHANCED PERSONNEL MANAGEMENT.—

(1)(A) The Director of National Intelligence shall, under regulations prescribed by the Director, provide incentives for personnel of elements of the intelligence community to serve—

- (i) on the staff of the Director of National Intelligence;
 - (ii) on the staff of the national intelligence centers;
 - (iii) on the staff of the National Counterterrorism Center;
- and

(iv) in other positions in support of the intelligence community management functions of the Director.

(B) Incentives under subparagraph (A) may include financial incentives, bonuses, and such other awards and incentives as the Director considers appropriate.

(2)(A) Notwithstanding any other provision of law, the personnel of an element of the intelligence community who are assigned or detailed under paragraph (1)(A) to service under the Director of National Intelligence shall be promoted at rates equivalent to or better than personnel of such element who are not so assigned or detailed.

(B) The Director may prescribe regulations to carry out this paragraph.

(3)(A) The Director of National Intelligence shall prescribe mechanisms to facilitate the rotation of personnel of the intelligence community through various elements of the intelligence community in the course of their careers in order to facilitate the widest possible understanding by such personnel of the variety of intelligence requirements, methods, users, and capabilities.

(B) The mechanisms prescribed under subparagraph (A) may include the following:

(i) The establishment of special occupational categories involving service, over the course of a career, in more than one element of the intelligence community.

(ii) The provision of rewards for service in positions undertaking analysis and planning of operations involving two or more elements of the intelligence community.

(iii) The establishment of requirements for education, training, service, and evaluation for service involving more than one element of the intelligence community.

(C) It is the sense of Congress that the mechanisms prescribed under this subsection should, to the extent practical, seek to duplicate for civilian personnel within the intelligence community the joint officer management policies established by chapter 38 of title 10, United States Code, and the other amendments made by title IV of the Goldwater-Nichols Department of Defense Reorganization Act of 1986 (Public Law 99-433).

(D) The mechanisms prescribed under subparagraph (A) and any other policies of the Director—

(i) may not require an employee of an office of inspector general for an element of the intelligence community,

including the Office of the Inspector General of the Intelligence Community, to rotate to a position in an office or organization of such an element over which such office of inspector general exercises jurisdiction; and

(ii) shall be implemented in a manner that exempts employees of an office of inspector general from a rotation that may impact the independence of such office.

(4)(A) Except as provided in subparagraph (B) and subparagraph (D), this subsection shall not apply with respect to personnel of the elements of the intelligence community who are members of the uniformed services.

(B) Mechanisms that establish requirements for education and training pursuant to paragraph (3)(B)(iii) may apply with respect to members of the uniformed services who are assigned to an element of the intelligence community funded through the National Intelligence Program, but such mechanisms shall not be inconsistent with personnel policies and education and training requirements otherwise applicable to members of the uniformed services.

(C) The personnel policies and programs developed and implemented under this subsection with respect to law enforcement officers (as that term is defined in section 5541(3) of title 5, United States Code) shall not affect the ability of law enforcement entities to conduct operations or, through the applicable chain of command, to control the activities of such law enforcement officers.

(D) Assignment to the Office of the Director of National Intelligence of commissioned officers of the Armed Forces shall be considered a joint-duty assignment for purposes of the joint officer management policies prescribed by chapter 38 of title 10, United States Code, and other provisions of that title.

(m) **ADDITIONAL AUTHORITY WITH RESPECT TO PERSONNEL.**—

(1) In addition to the authorities under subsection (f)(3), the Director of National Intelligence may exercise with respect to the personnel of the Office of the Director of National Intelligence any authority of the Director of the Central Intelligence Agency with respect to the personnel of the Central Intelligence Agency under the Central Intelligence Agency Act of 1949 [50 U.S.C. § 3501 et seq.], and other applicable provisions of law, as of the date of the enactment of this subsection to the same extent, and subject to the same conditions and limitations, that the

Director of the Central Intelligence Agency may exercise such authority with respect to personnel of the Central Intelligence Agency, including with respect to the notification requirement under section 8(c) of such Act (50 U.S.C. 3510(c)).

(2) Employees and applicants for employment of the Office of the Director of National Intelligence shall have the same rights and protections under the Office of the Director of National Intelligence as employees of the Central Intelligence Agency have under the Central Intelligence Agency Act of 1949, and other applicable provisions of law, as of the date of the enactment of this subsection.

(n) ACQUISITION AND OTHER AUTHORITIES.—

(1) In carrying out the responsibilities and authorities under this section, the Director of National Intelligence may exercise the acquisition and appropriations authorities referred to in the Central Intelligence Agency Act of 1949 [50 U.S.C. § 3501 et seq.] other than the authorities referred to in section 8(b) of that Act [50 U.S.C. § 3510(b)].

(2) For the purpose of the exercise of any authority referred to in paragraph (1), a reference to the head of an agency shall be deemed to be a reference to the Director of National Intelligence or the Principal Deputy Director of National Intelligence.

(3)(A) Any determination or decision to be made under an authority referred to in paragraph (1) by the head of an agency may be made with respect to individual purchases and contracts or with respect to classes of purchases or contracts, and shall be final.

(B) Except as provided in subparagraph (C), the Director of National Intelligence or the Principal Deputy Director of National Intelligence may, in such official's discretion, delegate to any officer or other official of the Office of the Director of National Intelligence any authority to make a determination or decision as the head of the agency under an authority referred to in paragraph (1).

(C) The limitations and conditions set forth in section 3(d) of the Central Intelligence Agency Act of 1949 [50 U.S.C. § 3503(d)] shall apply to the exercise by the Director of National Intelligence of an authority referred to in paragraph (1).

(D) Each determination or decision required by an authority referred to in the second sentence of section 3(d) of the Central Intelligence Agency Act of 1949 shall be based upon written findings made by the official making such determination or decision, which findings shall be final and shall be available within the Office of the Director of National Intelligence for a

period of at least six years following the date of such determination or decision.

(4)(A) In addition to the authority referred to in paragraph (1), the Director of National Intelligence may authorize the head of an element of the intelligence community to exercise an acquisition authority referred to in section 3 or 8(a) of the Central Intelligence Agency Act of 1949 [50 U.S.C. §§ 3503 and 3510(a)] for an acquisition by such element that is more than 50 percent funded under the National Intelligence Program.

(B) The head of an element of the intelligence community may not exercise an authority referred to in subparagraph (A) until—
(i) the head of such element (without delegation) submits to the Director of National Intelligence a written request that includes—

(I) a description of such authority requested to be exercised;

(II) an explanation of the need for such authority, including an explanation of the reasons that other authorities are insufficient; and

(III) a certification that the mission of such element would be—

(aa) impaired if such authority is not exercised; or

(bb) significantly and measurably enhanced if such authority is exercised; and

(ii) the Director of National Intelligence issues a written authorization that includes—

(I) a description of the authority referred to in subparagraph (A) that is authorized to be exercised; and

(II) a justification to support the exercise of such authority.

(C) A request and authorization to exercise an authority referred to in subparagraph (A) may be made with respect to an individual acquisition or with respect to a specific class of acquisitions described in the request and authorization referred to in subparagraph (B).

(D)(i) A request from a head of an element of the intelligence community located within one of the departments described in clause (ii) to exercise an authority referred to in subparagraph (A) shall be submitted to the Director of National Intelligence in

accordance with any procedures established by the head of such department.

(ii) The departments described in this clause are the Department of Defense, the Department of Energy, the Department of Homeland Security, the Department of Justice, the Department of State, and the Department of the Treasury.

(E)(i) The head of an element of the intelligence community may not be authorized to utilize an authority referred to in subparagraph (A) for a class of acquisitions for a period of more than 3 years, except that the Director of National Intelligence (without delegation) may authorize the use of such an authority for not more than 6 years.

(ii) Each authorization to utilize an authority referred to in subparagraph (A) may be extended in accordance with the requirements of subparagraph (B) for successive periods of not more than 3 years, except that the Director of National Intelligence (without delegation) may authorize an extension period of not more than 6 years.

(F) Subject to clauses (i) and (ii) of subparagraph (E), the Director of National Intelligence may only delegate the authority of the Director under subparagraphs (A) through (E) to the Principal Deputy Director of National Intelligence or a Deputy Director of National Intelligence.

(G) The Director of National Intelligence shall submit—

(i) to the congressional intelligence committees a notification of an authorization to exercise an authority referred to in subparagraph (A) or an extension of such authorization that includes the written authorization referred to in subparagraph (B)(ii); and

(ii) to the Director of the Office of Management and Budget a notification of an authorization to exercise an authority referred to in subparagraph (A) for an acquisition or class of acquisitions that will exceed \$50,000,000 annually.

(H) Requests and authorizations to exercise an authority referred to in subparagraph (A) shall remain available within the Office of the Director of National Intelligence for a period of at least 6 years following the date of such request or authorization.

(I) Nothing in this paragraph may be construed to alter or otherwise limit the authority of the Central Intelligence Agency to independently exercise an authority under section 3 or 8(a) of

NATIONAL SECURITY ACT OF 1947

the Central Intelligence Agency Act of 1949 [50 U.S.C. §§ 3503 and 3510(a)].

(5) Any authority provided to the Director of National Intelligence or the head of an element of the intelligence community pursuant to this subsection to make an expenditure referred to in subsection (a) of section 8 of the Central Intelligence Agency Act of 1949 (50 U.S.C. 3510) is subject to the notification requirement under subsection (c) of such section. If the Director of National Intelligence is required to make a notification for a specific expenditure pursuant to both this paragraph and paragraph (4)(G), the Director may make a single notification.

(6) OTHER TRANSACTION AUTHORITY.—

(A) In general. — In addition to other acquisition authorities, the Director of National Intelligence may exercise the acquisition authorities referred to in sections 4021 and 4022 of title 10, United States Code, subject to the provisions of this paragraph.

(B) DELEGATION.—

(i) The Director shall delegate the authorities provided by subparagraph (A) to the heads of elements of the intelligence community.

(ii) The heads of elements of the intelligence community shall, to the maximum extent practicable, delegate the authority delegated under clause (i) to the official of the respective element of the intelligence community responsible for decisions with respect to basic, applied, or advanced research activities or the adoption of such activities within such element.

(C) INTELLIGENCE COMMUNITY AUTHORITY.—

(i) For purposes of this paragraph, the limitation in section 4022(a)(1) of title 10, United States Code, shall not apply to elements of the intelligence community.

(ii) Subject to section 4022(a)(2) of such title, the Director may enter into transactions and agreements (other than contracts, cooperative agreements, and grants) of amounts not to exceed \$75,000,000 under this paragraph to carry out basic, applied, and advanced research projects and prototype projects in support of intelligence activities.

(iii) For purposes of this paragraph, the limitations specified in section 4022(a)(2) of such title shall apply to the intelligence community in lieu of the Department of Defense, and the Director shall—

(I) identify appropriate officials who can make the determinations required in subparagraph (B)(i) of such section for the intelligence community; and
(II) brief the congressional intelligence committees, the Subcommittee on Defense of the Committee on Appropriations of the Senate, and the Subcommittee on Defense of the Committee on Appropriations of the House of Representatives in lieu of the congressional defense committees, as specified in subparagraph (B)(ii) of such section.

(iv) For purposes of this paragraph, the limitation in section 4022(a)(3) of such title shall not apply to elements of the intelligence community.

(v) In carrying out this paragraph, section 4022(d)(1) of such title shall be applied by substituting “Director of National Intelligence” for “Secretary of Defense”.

(vi) For purposes of this paragraph, the limitations in section 4022(d)(2) of such title shall not apply to elements of the intelligence community.

(vii) In addition to the follow-on production contract criteria in section 4022(f)(2) of such title, the following additional criteria shall apply:

(I) The authorizing official of the relevant element of the intelligence community determines that Government users of the proposed production product or production service have been consulted.

(II) In the case of a proposed production product that is software, there are mechanisms in place for Government users to provide ongoing feedback to participants to the follow-on production contract.

(III) In the case of a proposed production product that is software, there are mechanisms in place to promote the interoperability and accessibility with and between Government and commercial software providers, including by the promotion of open application programming interfaces and requirement of appropriate software documentation.

(IV) The award follows a documented market analysis as mandated by the Federal Acquisition Regulations surveying available and comparable products.

(V) In the case of a proposed production product that is software, the follow-on production contract includes a

requirement that, for the duration of such contract (or such other period of time as may be agreed to as a term of such contract)—

(aa) the participants provide the most up-to-date version of the product that is available in the commercial marketplace and is consistent with security requirements;

(bb) there are mechanisms in place for the participants to provide timely updates to the production product; and

(cc) the authority specified in section 4022(f)(5) of such title shall be exercised by the Director in lieu of the Secretary of Defense.

(D) IMPLEMENTATION POLICY. —The Director, in consultation with the heads of the elements of the intelligence community, shall—

(i) not later than 180 days after the date of the enactment of the Intelligence Authorization Act for Fiscal Year 2023, establish and implement an intelligence community-wide policy prescribing the use and limitations of the authority under this paragraph, particularly with respect to the application of subparagraphs (B) and (C);

(ii) periodically review and update the policy established under clause (i); and

(iii) submit to the congressional intelligence committees, the Committee on Appropriations of the Senate, and the Committee on Appropriations of the House of Representatives the policy when established under clause (i) or updated under clause (ii).

(E) ANNUAL REPORT.—

(i) IN GENERAL. —Not less frequently than annually, the Director shall submit to the congressional intelligence committees, the Committee on Appropriations of the Senate, and the Committee on Appropriations of the House of Representatives a report detailing the use by the intelligence community of the authority provided by this paragraph.

(ii) ELEMENTS.—

(I) Required elements.—Each report required by clause

(i) shall detail the following:

(aa) The number of transactions.

(bb) The participants to such transactions.

(cc) The purpose of the transaction.

NATIONAL SECURITY ACT OF 1947

- (dd) The amount of each transaction.
- (ee) Concerns with the efficiency of the policy.
- (ff) Any recommendations for how to improve the process.

(II) Other elements.—Each report required by clause (i) may describe such transactions which have been awarded follow-on production contracts either pursuant to the authority provided by this paragraph or another acquisition authority available to the intelligence community.'

(o) CONSIDERATION OF VIEWS OF ELEMENTS OF INTELLIGENCE COMMUNITY.— In carrying out the duties and responsibilities under this section, the Director of National Intelligence shall take into account the views of a head of a department containing an element of the intelligence community and of the Director of the Central Intelligence Agency.

(p) CERTAIN RESPONSIBILITIES OF DIRECTOR OF NATIONAL INTELLIGENCE RELATING TO NATIONAL INTELLIGENCE PROGRAM.—

(1) Subject to the direction of the President, the Director of National Intelligence shall, after consultation with the Secretary of Defense, ensure that the National Intelligence Program budgets for the elements of the intelligence community that are within the Department of Defense are adequate to satisfy the national intelligence needs of the Department of Defense, including the needs of the Chairman of the Joint Chiefs of Staff and the commanders of the unified and specified commands, and wherever such elements are performing Government-wide functions, the needs of other Federal departments and agencies.

(2) Consistent with subsection (c)(5)(C), the Director of National Intelligence shall, after consultation with the Director of the Federal Bureau of Investigation, ensure that the programs and activities of the Federal Bureau of Investigation that are part of the National Intelligence Program are executed in a manner that conforms with the requirements of the national intelligence strategy under section 108A of this Act and the National Intelligence Priorities Framework of the Office of the Director of National Intelligence (or any successor mechanism established for the prioritization of such programs and activities).

(3) Not later than March 1 of each year, the President, acting through the Director of National Intelligence, shall submit to the congressional intelligence committees, the Subcommittee on Defense of the Committee on Appropriations of the Senate, and the Subcommittee on Defense of the Committee on Appropriations of the House of Representatives a copy of the most recently updated National Intelligence Priorities Framework

of the Office of the Director of National Intelligence (or any such successor mechanism).

(q) ACQUISITIONS OF MAJOR SYSTEMS.—

(1) For each intelligence program within the National Intelligence Program for the acquisition of a major system, the Director of National Intelligence shall—

(A) require the development and implementation of a program management plan that includes cost, schedule, security risks, and performance goals and program milestone criteria, except that with respect to Department of Defense programs the Director shall consult with the Secretary of Defense;

(B) serve as exclusive milestone decision authority, except that with respect to Department of Defense programs the Director shall serve as milestone decision authority jointly with the Secretary of Defense or the designee of the Secretary; and

(C) periodically—

(i) review and assess the progress made toward the achievement of the goals and milestones established in such plan; and

(ii) submit to Congress a report on the results of such review and assessment.

(2) If the Director of National Intelligence and the Secretary of Defense are unable to reach an agreement on a milestone decision under paragraph (1)(B), the President shall resolve the conflict.

(3) Nothing in this subsection may be construed to limit the authority of the Director of National Intelligence to delegate to any other official any authority to perform the responsibilities of the Director under this subsection.

(4) In this subsection:

(A) The term “intelligence program”, with respect to the acquisition of a major system, means a program that—

(i) is carried out to acquire such major system for an element of the intelligence community; and

(ii) is funded in whole out of amounts available for the National Intelligence Program.

(B) The term “major system” has the meaning given such term in section 4(9) of the Federal Property and Administrative Services Act of 1949 [41 U.S.C. § 109].

(r) PERFORMANCE OF COMMON SERVICES.—The Director of National Intelligence shall, in consultation with the heads of departments and agencies of the United States Government containing elements within the intelligence community and with the Director of the Central Intelligence Agency, coordinate

the performance by the elements of the intelligence community within the National Intelligence Program of such services as are of common concern to the intelligence community, which services the Director of National Intelligence determines can be more efficiently accomplished in a consolidated manner.

(s) PAY AUTHORITY FOR CRITICAL POSITIONS.—

(1) Notwithstanding any pay limitation established under any other provision of law applicable to employees in elements of the intelligence community, the Director of National Intelligence may, in coordination with the Director of the Office of Personnel Management and the Director of the Office of Management and Budget, grant authority to the head of a department or agency to fix the rate of basic pay for one or more positions within the intelligence community at a rate in excess of any applicable limitation, subject to the provisions of this subsection. The exercise of authority so granted is at the discretion of the head of the department or agency employing the individual in a position covered by such authority, subject to the provisions of this subsection and any conditions established by the Director of National Intelligence when granting such authority.

(2) Authority under this subsection may be granted or exercised only—

- (A) with respect to a position that requires an extremely high level of expertise and is critical to successful accomplishment of an important mission; and
- (B) to the extent necessary to recruit or retain an individual exceptionally well qualified for the position.

(3) The head of a department or agency may not fix a rate of basic pay under this subsection at a rate greater than the rate payable for level II of the Executive Schedule under section 5313 of title 5, United States Code, except upon written approval of the Director of National Intelligence or as otherwise authorized by law.

(4) The head of a department or agency may not fix a rate of basic pay under this subsection at a rate greater than the rate payable for level I of the Executive Schedule under section 5312 of title 5, United States Code, except upon written approval of the President in response to a request by the Director of National Intelligence or as otherwise authorized by law.

(5) Any grant of authority under this subsection for a position shall terminate at the discretion of the Director of National Intelligence.

(6)(A) The Director of National Intelligence shall notify the congressional intelligence committees not later than 30 days after the date on which the Director grants authority to the head of a department or agency under this subsection.

(B) The head of a department or agency to which the Director of National Intelligence grants authority under this subsection shall

notify the congressional intelligence committees and the Director of the exercise of such authority not later than 30 days after the date on which such head exercises such authority.

(t) AWARD OF RANK TO MEMBERS OF THE SENIOR NATIONAL INTELLIGENCE SERVICE.—

(1) The President, based on the recommendation of the Director of National Intelligence, may award a rank to a member of the Senior National Intelligence Service or other intelligence community senior civilian officer not already covered by such a rank award program in the same manner in which a career appointee of an agency may be awarded a rank under section 4507 of title 5, United States Code.

(2) The President may establish procedures to award a rank under paragraph (1) to a member of the Senior National Intelligence Service or a senior civilian officer of the intelligence community whose identity as such a member or officer is classified information (as defined in section 606(1)).

(u) CONFLICT OF INTEREST REGULATIONS.—The Director of National Intelligence, in consultation with the Director of the Office of Government Ethics, shall issue regulations prohibiting an officer or employee of an element of the intelligence community from engaging in outside employment if such employment creates a conflict of interest or appearance thereof.

(v) AUTHORITY TO ESTABLISH POSITIONS IN EXCEPTED SERVICE.—

(1) The Director of National Intelligence, with the concurrence of the head of the covered department concerned and in consultation with the Director of the Office of Personnel Management, may—

(A) convert competitive service positions, and the incumbent of such positions, within an element of the intelligence community in such department, to excepted service positions as the Director of National Intelligence determines necessary to carry out the intelligence functions of such element; and

(B) establish new positions in the excepted service within an element of the intelligence community in such department, if the Director of National Intelligence determines such positions are necessary to carry out the intelligence functions of such element.

(2) An incumbent occupying a position on the date of the enactment of the Intelligence Authorization Act for Fiscal Year 2012 selected to be converted to the excepted service under this section shall have the right to refuse such conversion. Once such individual no longer occupies the position, the position may be converted to the excepted service.

(3) A covered department may appoint an individual to a position converted or established pursuant to this subsection without regard to the

civil-service laws, including parts II and III of title 5, United States Code.

(4) In this subsection, the term “covered department” means the Department of Energy, the Department of Homeland Security, the Department of State, or the Department of the Treasury.

(w) NUCLEAR PROLIFERATION ASSESSMENT STATEMENTS INTELLIGENCE COMMUNITY ADDENDUM.—The Director of National Intelligence, in consultation with the heads of the appropriate elements of the intelligence community and the Secretary of State, shall provide to the President, the congressional intelligence committees, the Committee on Foreign Affairs of the House of Representatives, and the Committee on Foreign Relations of the Senate an addendum to each Nuclear Proliferation Assessment Statement accompanying a civilian nuclear cooperation agreement, containing a comprehensive analysis of the country’s export control system with respect to nuclear-related matters, including interactions with other countries of proliferation concern and the actual or suspected nuclear, dual-use, or missile-related transfers to such countries.

(x) REQUIREMENTS FOR INTELLIGENCE COMMUNITY CONTRACTORS.—The Director of National Intelligence, in consultation with the heads of the elements of the intelligence community, shall—

(1) ensure that—

(A) any contractor to an element of the intelligence community with access to a classified network or classified information develops and operates a security plan that is consistent with standards established by the Director of National Intelligence for intelligence community networks; and

(B) each contract awarded by an element of the intelligence community includes provisions requiring the contractor comply with such plan and such standards;

(2) conduct periodic assessments of each security plan required under paragraph (1)(A) to ensure such security plan complies with the requirements of such paragraph; and

(3) ensure that the insider threat detection capabilities and insider threat policies of the intelligence community, including the policy under subsection (f)(8), apply to facilities of contractors with access to a classified network.

(y) FUNDRAISING.—

(1) The Director of National Intelligence may engage in fundraising in an official capacity for the benefit of nonprofit organizations that—

(A) provide support to surviving family members of a deceased employee of an element of the intelligence community; or

(B) otherwise provide support for the welfare, education, or recreation of employees of an element of the intelligence

community, former employees of an element of the intelligence community, or family members of such employees.

(2) In this subsection, the term “fundraising” means the raising of funds through the active participation in the promotion, production, or presentation of an event designed to raise funds and does not include the direct solicitation of money by any other means.

(3) Not later than 7 days after the date the Director engages in fundraising authorized by this subsection or at the time the decision is made to participate in such fundraising, the Director shall notify the congressional intelligence committees of such fundraising.

(4) The Director, in consultation with the Director of the Office of Government Ethics, shall issue regulations to carry out the authority provided in this subsection. Such regulations shall ensure that such authority is exercised in a manner that is consistent with all relevant ethical constraints and principles, including the avoidance of any prohibited conflict of interest or appearance of impropriety.

(z) ANALYSES AND IMPACT STATEMENTS REGARDING PROPOSED INVESTMENT INTO THE UNITED STATES.—

(1) Not later than 20 days after the completion of a review or an investigation of any proposed investment into the United States for which the Director has prepared analytic materials, the Director shall submit to the Select Committee on Intelligence of the Senate and the Permanent Select Committee on Intelligence of the House of Representative copies of such analytic materials, including any supplements or amendments to such analysis made by the Director.

(2) Not later than 60 days after the completion of consideration by the United States Government of any investment described in paragraph (1), the Director shall determine whether such investment will have an operational impact on the intelligence community, and, if so, shall submit a report on such impact to the Select Committee on Intelligence of the Senate and the Permanent Select Committee on Intelligence of the House of Representatives. Each such report shall—

(A) describe the operational impact of the investment on the intelligence community; and

(B) describe any actions that have been or will be taken to mitigate such impact.

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

SEC. 103. [50 U.S.C. § 3025]

(a) OFFICE OF DIRECTOR OF NATIONAL INTELLIGENCE.—There is an Office of the Director of National Intelligence.

(b) **FUNCTION.**—The function of the Office of the Director of National Intelligence is to assist the Director of National Intelligence in carrying out the duties and responsibilities of the Director under this Act and other applicable provisions of law, and to carry out such other duties as may be prescribed by the President or by law.

(c) **COMPOSITION.**—The Office of the Director of National Intelligence is composed of the following:

- (1) The Director of National Intelligence.
- (2) The Principal Deputy Director of National Intelligence.
- (3) Any Deputy Director of National Intelligence appointed under section 103A.
- (4) The National Intelligence Council.
- (5) The General Counsel.
- (6) The Civil Liberties Protection Officer.
- (7) The Director of Science and Technology.
- (8) The Director of the National Counterintelligence and Security Center.
- (9) The Chief Information Officer of the Intelligence Community.
- (10) The Inspector General of the Intelligence Community.
- (11) The Director of the National Counterterrorism Center.
- (12) The Director of the National Counterproliferation [and Biosecurity] Center.
- (13) The Chief Financial Officer of the Intelligence Community.
- (14) Such other offices and officials as may be established by law or the Director may establish or designate in the Office, including national intelligence centers.

(d) **STAFF.**—

(1) To assist the Director of National Intelligence in fulfilling the duties and responsibilities of the Director, the Director shall employ and utilize in the Office of the Director of National Intelligence a professional staff having an expertise in matters relating to such duties and responsibilities, and may establish permanent positions and appropriate rates of pay with respect to that staff.

(2) The staff of the Office of the Director of National Intelligence under paragraph (1) shall include the staff of the Office of the Deputy Director of Central Intelligence for Community Management that is transferred to the Office of the Director of National Intelligence under section 1091 of the National Security Intelligence Reform Act of 2004.

(e) **TEMPORARY FILLING OF VACANCIES.**—With respect to filling temporarily a vacancy in an office within the Office of the Director of National Intelligence (other than that of the Director of National Intelligence), section 3345(a)(3) of title 5, United States Code, may be applied—

(1) in the matter preceding subparagraph (A), by substituting “an element of the intelligence community, as that term is defined in section 3(4) of the National Security Act of 1947 [50 U.S.C. § 401a(4)],” for “such Executive agency”; and

(2) in subparagraph (A), by substituting “the intelligence community” for “such agency”.

(f) **LOCATION OF THE OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE.**— The headquarters of the Office of the Director of National Intelligence may be located in the Washington metropolitan region, as that term is defined in section 8301 of title 40, United States Code.

DEPUTY DIRECTORS OF NATIONAL INTELLIGENCE

SEC. 103A. [50 U.S.C. § 3026]

(a) **PRINCIPAL DEPUTY DIRECTOR OF NATIONAL INTELLIGENCE.**—

(1) There is a Principal Deputy Director of National Intelligence who shall be appointed by the President, by and with the advice and consent of the Senate.

(2) In the event of a vacancy in the position of Principal Deputy Director of National Intelligence, the Director of National Intelligence shall recommend to the President an individual for appointment as Principal Deputy Director of National Intelligence.

(3) Any individual nominated for appointment as Principal Deputy Director of National Intelligence shall have extensive national security experience and management expertise.

(4) The individual serving as Principal Deputy Director of National Intelligence shall not, while so serving, serve in any capacity in any other element of the intelligence community.

(5) The Principal Deputy Director of National Intelligence shall assist the Director of National Intelligence in carrying out the duties and responsibilities of the Director.

(6) The Principal Deputy Director of National Intelligence shall act for, and exercise the powers of, the Director of National Intelligence during the absence or disability of the Director of National Intelligence or during a vacancy in the position of Director of National Intelligence.

(b) **DEPUTY DIRECTORS OF NATIONAL INTELLIGENCE.**—

(1) There may be not more than four Deputy Directors of National Intelligence who shall be appointed by the Director of National Intelligence.

(2) Each Deputy Director of National Intelligence appointed under this subsection shall have such duties, responsibilities, and authorities as the Director of National Intelligence may assign or are specified by law.

(c) **MILITARY STATUS OF DIRECTOR OF NATIONAL INTELLIGENCE AND PRINCIPAL DEPUTY DIRECTOR OF NATIONAL INTELLIGENCE.**—

- (1) Not more than one of the individuals serving in the positions specified in paragraph (2) may be a commissioned officer of the Armed Forces in active status.
- (2) The positions referred to in this paragraph are the following:
 - (A) The Director of National Intelligence.
 - (B) The Principal Deputy Director of National Intelligence.
- (3) It is the sense of Congress that, under ordinary circumstances, it is desirable that one of the individuals serving in the positions specified in paragraph (2)—
 - (A) be a commissioned officer of the Armed Forces, in active status; or
 - (B) have, by training or experience, an appreciation of military intelligence activities and requirements.
- (4) A commissioned officer of the Armed Forces, while serving in a position specified in paragraph (2)—
 - (A) shall not be subject to supervision or control by the Secretary of Defense or by any officer or employee of the Department of Defense;
 - (B) shall not exercise, by reason of the officer's status as a commissioned officer, any supervision or control with respect to any of the military or civilian personnel of the Department of Defense except as otherwise authorized by law; and
 - (C) shall not be counted against the numbers and percentages of commissioned officers of the rank and grade of such officer authorized for the military department of that officer.
- (5) Except as provided in subparagraph (A) or (B) of paragraph (4), the appointment of an officer of the Armed Forces to a position specified in paragraph (2) shall not affect the status, position, rank, or grade of such officer in the Armed Forces, or any emolument, perquisite, right, privilege, or benefit incident to or arising out of such status, position, rank, or grade.
- (6) A commissioned officer of the Armed Forces on active duty who is appointed to a position specified in paragraph (2), while serving in such position and while remaining on active duty, shall continue to receive military pay and allowances and shall not receive the pay prescribed for such position. Funds from which such pay and allowances are paid shall be reimbursed from funds available to the Director of National Intelligence.

NATIONAL SECURITY ACT OF 1947

SEC. 103B. [50 U.S.C. § 3027]

(a) NATIONAL INTELLIGENCE COUNCIL.—There is a National Intelligence Council.

(b) COMPOSITION.—

(1) The National Intelligence Council shall be composed of senior analysts within the intelligence community and substantive experts from the public and private sector, who shall be appointed by, report to, and serve at the pleasure of, the Director of National Intelligence.

(2) The Director shall prescribe appropriate security requirements for personnel appointed from the private sector as a condition of service on the Council, or as contractors of the Council or employees of such contractors, to ensure the protection of intelligence sources and methods while avoiding, wherever possible, unduly intrusive requirements which the Director considers to be unnecessary for this purpose.

(c) DUTIES AND RESPONSIBILITIES.—

(1) The National Intelligence Council shall—

(A) produce national intelligence estimates for the United States Government, including alternative views held by elements of the intelligence community and other information as specified in paragraph (2);

(B) evaluate community-wide collection and production of intelligence by the intelligence community and the requirements and resources of such collection and production; and

(C) otherwise assist the Director of National Intelligence in carrying out the responsibilities of the Director under section 102A.

(2) The Director of National Intelligence shall ensure that the Council satisfies the needs of policymakers and other consumers of intelligence.

(d) SERVICE AS SENIOR INTELLIGENCE ADVISERS.—Within their respective areas of expertise and under the direction of the Director of National Intelligence, the members of the National Intelligence Council shall constitute the senior intelligence advisers of the intelligence community for purposes of representing the views of the intelligence community within the United States Government.

(e) AUTHORITY TO CONTRACT.—Subject to the direction and control of the Director of National Intelligence, the National Intelligence Council may carry out its responsibilities under this section by contract, including contracts for substantive experts necessary to assist the Council with particular assessments under this section.

(f) STAFF.—The Director of National Intelligence shall make available to the National Intelligence Council such staff as may be necessary to permit the Council to carry out its responsibilities under this section.

(g) AVAILABILITY OF COUNCIL AND STAFF.—

(1) The Director of National Intelligence shall take appropriate measures to ensure that the National Intelligence Council and its staff satisfy the needs of policymaking officials and other consumers of intelligence.

(2) The Council shall be readily accessible to policymaking officials and other appropriate individuals not otherwise associated with the intelligence community.

(h) SUPPORT.—The heads of the elements of the intelligence community shall, as appropriate, furnish such support to the National Intelligence Council, including the preparation of intelligence analyses, as may be required by the Director of National Intelligence.

(i) NATIONAL INTELLIGENCE COUNCIL PRODUCT.—For purposes of this section, the term “National Intelligence Council product” includes a National Intelligence Estimate and any other intelligence community assessment that sets forth the judgment of the intelligence community as a whole on a matter covered by such product.

GENERAL COUNSEL

SEC. 103C. [50 U.S.C. § 3028]

(a) GENERAL COUNSEL.—There is a General Counsel of the Office of the Director of National Intelligence who shall be appointed by the President, by and with the advice and consent of the Senate.

(b) PROHIBITION ON DUAL SERVICE AS GENERAL COUNSEL OF ANOTHER AGENCY.—The individual serving in the position of General Counsel may not, while so serving, also serve as the General Counsel of any other department, agency, or element of the United States Government.

(c) SCOPE OF POSITION.—The General Counsel is the chief legal officer of the Office of the Director of National Intelligence.

(d) FUNCTIONS.—The General Counsel shall perform such functions as the Director of National Intelligence may prescribe.

CIVIL LIBERTIES PROTECTION OFFICER

SEC. 103D. [50 U.S.C. § 3029]

(a) CIVIL LIBERTIES PROTECTION OFFICER.—

(1) Within the Office of the Director of National Intelligence, there is a Civil Liberties Protection Officer who shall be appointed by the Director of National Intelligence.

(2) The Civil Liberties Protection Officer shall report directly to the Director of National Intelligence.

(b) DUTIES.—The Civil Liberties Protection Officer shall—

- (1) ensure that the protection of civil liberties and privacy is appropriately incorporated in the policies and procedures developed for and implemented by the Office of the Director of National Intelligence and the elements of the intelligence community within the National Intelligence Program;
- (2) oversee compliance by the Office and the Director of National Intelligence with requirements under the Constitution and all laws, regulations, Executive orders, and implementing guidelines relating to civil liberties and privacy;
- (3) review and assess complaints and other information indicating possible abuses of civil liberties and privacy in the administration of the programs and operations of the Office and the Director of National Intelligence and, as appropriate, investigate any such complaint or information;
- (4) ensure that the use of technologies sustain, and do not erode, privacy protections relating to the use, collection, and disclosure of personal information;
- (5) ensure that personal information contained in a system of records subject to section 552a of title 5, United States Code (popularly referred to as the “Privacy Act”), is handled in full compliance with fair information practices as set out in that section;
- (6) conduct privacy impact assessments when appropriate or as required by law; and
- (7) perform such other duties as may be prescribed by the Director of National Intelligence or specified by law.

(c) **USE OF AGENCY INSPECTORS GENERAL.**—When appropriate, the Civil Liberties Protection Officer may refer complaints to the Office of Inspector General having responsibility for the affected element of the department or agency of the intelligence community to conduct an investigation under paragraph (3) of subsection (b).

DIRECTOR OF SCIENCE AND TECHNOLOGY

SEC. 103E. [50 U.S.C. § 3030]

(a) **DIRECTOR OF SCIENCE AND TECHNOLOGY.**—There is a Director of Science and Technology within the Office of the Director of National Intelligence who shall be appointed by the Director of National Intelligence.

(b) **REQUIREMENT RELATING TO APPOINTMENT.**—An individual appointed as Director of Science and Technology shall have a professional background and experience appropriate for the duties of the Director of Science and Technology. In making such appointment, the Director of National Intelligence may give

preference to an individual with experience outside of the United States Government.

(c) DUTIES.—The Director of Science and Technology shall—

- (1) act as the chief representative of the Director of National Intelligence for science and technology;
- (2) chair the Director of National Intelligence Science and Technology Committee under subsection (d);
- (3) assist the Director in formulating a long-term strategy for scientific advances in the field of intelligence;
- (4) assist the Director on the science and technology elements of the budget of the Office of the Director of National Intelligence; and
- (5) perform other such duties as may be prescribed by the Director of National Intelligence or specified by law.

(d) DIRECTOR OF NATIONAL INTELLIGENCE SCIENCE AND TECHNOLOGY COMMITTEE.—

- (1) There is within the Office of the Director of Science and Technology a Director of National Intelligence Science and Technology Committee.
- (2) The Committee shall be composed of the principal science officers of the National Intelligence Program.
- (3) The Committee shall—
 - (A) coordinate advances in research and development related to intelligence; and
 - (B) perform such other functions as the Director of Science and Technology shall prescribe.

**DIRECTOR OF THE NATIONAL COUNTERINTELLIGENCE
AND SECURITY CENTER**

SEC. 103F. [50 U.S.C. § 3031]

(a) DIRECTOR OF THE NATIONAL COUNTERINTELLIGENCE AND SECURITY CENTER.—The Director of the National Counterintelligence and Security Center appointed under section 902 of the Counterintelligence Enhancement Act of 2002 (50 U.S.C. 3382) is a component of the Office of the Director of National Intelligence.

(b) DUTIES.—The Director of the National Counterintelligence and Security Center shall perform the duties provided in the Counterintelligence Enhancement Act of 2002 and such other duties as may be prescribed by the Director of National Intelligence or specified by law.

CHIEF INFORMATION OFFICER

SEC. 103G. [50 U.S.C. § 3032]

(a) **CHIEF INFORMATION OFFICER.**—To assist the Director of National Intelligence in carrying out the responsibilities of the Director under this Act and other applicable provisions of law, there shall be within the Office of the Director of National Intelligence a Chief Information Officer of the Intelligence Community who shall be appointed by the Director. The Chief Information Officer shall report directly to the Director of National Intelligence.

(b) **DUTIES AND RESPONSIBILITIES.**—Subject to the direction of the Director of National Intelligence, the Chief Information Officer of the Intelligence Community shall—

- (1) manage activities relating to the information technology infrastructure and enterprise architecture requirements of the intelligence community;
- (2) have procurement approval authority over all information technology items related to the enterprise architectures of all intelligence community components;
- (3) direct and manage all information technology-related procurement for the intelligence community; and
- (4) ensure that all expenditures for information technology and research and development activities are consistent with the intelligence community enterprise architecture and the strategy of the Director for such architecture.

(c) **PROHIBITION ON SIMULTANEOUS SERVICE AS OTHER CHIEF INFORMATION OFFICER.**—An individual serving in the position of Chief Information Officer of the Intelligence Community may not, while so serving, serve as the chief information officer of any other department or agency, or component thereof, of the United States Government.

(d) **PROHIBITION ON SIMULTANEOUS SERVICE AS CHIEF DATA OFFICER AND CHIEF INFORMATION OFFICER.**—An individual serving in the position of Chief Information Officer of the Intelligence Community or chief information officer of any other element of the intelligence community shall not concurrently serve as the Intelligence Community Chief Data Officer under section 103K and as the chief data officer of any other element of the intelligence community.

INSPECTOR GENERAL OF THE INTELLIGENCE COMMUNITY

SEC. 103H. [50 U.S.C. § 3033]

(a) **OFFICE OF INSPECTOR GENERAL OF THE INTELLIGENCE COMMUNITY.**—There is within the Office of the Director of National Intelligence an Office of the Inspector General of the Intelligence Community.

(b) PURPOSE.—The purpose of the Office of the Inspector General of the Intelligence Community is—

- (1) to create an objective and effective office, appropriately accountable to Congress, to initiate and conduct independent investigations, inspections, audits, and reviews on programs and activities within the responsibility and authority of the Director of National Intelligence;
- (2) to provide leadership and coordination and recommend policies for activities designed—

- (A) to promote economy, efficiency, and effectiveness in the administration and implementation of such programs and activities; and

- (B) to prevent and detect fraud and abuse in such programs and activities;

- (3) to provide a means for keeping the Director of National Intelligence fully and currently informed about—

- (A) problems and deficiencies relating to the administration of programs and activities within the responsibility and authority of the Director of National Intelligence; and

- (B) the necessity for, and the progress of, corrective actions; and

- (4) in the manner prescribed by this section, to ensure that the congressional intelligence committees are kept similarly informed of—

- (A) significant problems and deficiencies relating to programs and activities within the responsibility and authority of the Director of National Intelligence; and

- (B) the necessity for, and the progress of, corrective actions.

(c) INSPECTOR GENERAL OF THE INTELLIGENCE COMMUNITY.—

- (1) There is an Inspector General of the Intelligence Community, who shall be the head of the Office of the Inspector General of the Intelligence Community, who shall be appointed by the President, by and with the advice and consent of the Senate.

- (2) The nomination of an individual for appointment as Inspector General shall be made—

- (A) without regard to political affiliation;

- (B) on the basis of integrity, compliance with security standards of the intelligence community, and prior experience in the field of intelligence or national security; and

- (C) on the basis of demonstrated ability in accounting, financial analysis, law, management analysis, public administration, or investigations.

- (3) The Inspector General shall report directly to and be under the general supervision of the Director of National Intelligence.

(4)(A) The Inspector General may be removed from office only by the President. The President shall communicate in writing to the congressional intelligence committees the substantive rationale, including detailed and case-specific reasons, for the removal not later than 30 days prior to the effective date of such removal. Nothing in this paragraph shall be construed to prohibit a personnel action otherwise authorized by law, other than transfer or removal.

(B) If there is an open or completed inquiry into the Inspector General that relates to the removal or transfer of the Inspector General under subparagraph (A), the written communication required under that subparagraph shall—

(i) identify each entity that is conducting, or that conducted, the inquiry; and

(ii) in the case of a completed inquiry, contain the findings made during the inquiry.

(5)(A) Subject to the other provisions of this paragraph, only the President may place the Inspector General on nonduty status.

(B) If the President places the Inspector General on nonduty status, the President shall communicate in writing the substantive rationale, including detailed and case-specific reasons, for the change in status to the congressional intelligence committees not later than 15 days before the date on which the change in status takes effect, except that the President may submit that communication not later than the date on which the change in status takes effect if—

(i) the President has made a determination that the continued presence of the Inspector General in the workplace poses a threat described in any of clauses (i) through (iv) of section 6329b(b)(2)(A) of title 5, United States Code; and

(ii) in the communication, the President includes a report on the determination described in clause (i), which shall include—

(I) a specification of which clause of section 6329b(b)(2)(A) of title 5, United States Code, the President has determined applies under clause (i);

(II) the substantive rationale, including detailed and case-specific reasons, for the determination made under clause (i);

(III) an identification of each entity that is conducting, or that conducted, any inquiry upon which the determination under clause (i) was made; and

- (IV) in the case of an inquiry described in subclause (III) that is completed, the findings made during that inquiry.
- (C) The President may not place the Inspector General on nonduty status during the 30-day period preceding the date on which the Inspector General is removed or transferred under paragraph (4)(A) unless the President—
- (i) has made a determination that the continued presence of the Inspector General in the workplace poses a threat described in any of clauses (i) through (iv) of section 6329b(b)(2)(A) of title 5, United States Code; and
 - (ii) not later than the date on which the change in status takes effect, submits to the congressional intelligence committees a written communication that contains the information required under subparagraph (B), including the report required under clause (ii) of that subparagraph.
- (6)(A) In this subsection, the term “first assistant to the position of Inspector General” has the meaning given in section 3 of the Inspector General Act of 1978 (5 U.S.C. App.).
- (B) If the Inspector General dies, resigns, or is otherwise unable to perform the functions and duties of the position—
- (i) section 3345(a) of title 5, United States Code, and section 103(e) of the National Security Act of 1947 (50 U.S.C. 3024(e)) shall not apply;
 - (ii) subject to subparagraph (D), the first assistant to the position of Inspector General shall perform the functions and duties of the Inspector General temporarily in an acting capacity subject to the time limitations of section 3346 of title 5, United States Code; and
 - (iii) notwithstanding clause (ii), and subject to subparagraphs (D) and (E), the President (and only the President) may direct an officer or employee of any Office of an Inspector General to perform the functions and duties of the Inspector General temporarily in an acting capacity subject to the time limitations of section 3346 of title 5, United States Code, only if—
- (I) during the 365-day period preceding the date of death, resignation, or beginning of inability to serve of the Inspector General, the officer or employee served in a position in an Office of an Inspector General for not less than 90 days, except that—
- (aa) the requirement under this subclause shall not apply if the officer is an Inspector General; and

(bb) for the purposes of this clause, performing the functions and duties of an Inspector General temporarily in an acting capacity does not qualify as service in a position in an Office of an Inspector General;

(II) the rate of pay for the position of the officer or employee described in subclause (I) is equal to or greater than the minimum rate of pay payable for a position at GS-15 of the General Schedule;

(III) the officer or employee has demonstrated ability in accounting, auditing, financial analysis, law, management analysis, public administration, or investigations; and

(IV) not later than 30 days before the date on which the direction takes effect, the President communicates in writing to the congressional intelligence committees the substantive rationale, including the detailed and case-specific reasons, for such direction, including the reason for the direction that someone other than the individual who is performing the functions and duties of the Inspector General temporarily in an acting capacity (as of the date on which the President issues that direction) perform those functions and duties temporarily in an acting capacity.

(C) Notwithstanding section 3345(a) of title 5, United States Code, section 103(e) of the National Security Act of 1947 (50 U.S.C. 3025(e)), and clauses (ii) and (iii) of subparagraph (B), and subject to subparagraph (D), during any period in which the Inspector General is on nonduty status—

(i) the first assistant to the position of Inspector General shall perform the functions and duties of the position temporarily in an acting capacity subject to the time limitations of section 3346 of title 5, United States Code; and

(ii) if the first assistant described in clause (i) dies, resigns, or becomes otherwise unable to perform those functions and duties, the President (and only the President) may direct an officer or employee in the Office of Inspector General to perform those functions and duties temporarily in an acting capacity, subject to the time limitations of section 3346 of title 5, United States Code, if—

(I) that direction satisfies the requirements under subclauses (II), (III), and (IV) of subparagraph (B)(iii); and

(II) that officer or employee served in a position in that Office of Inspector General for not fewer than 90 of the 365 days preceding the date on which the President makes that direction.

(D) An individual may perform the functions and duties of the Inspector General temporarily and in an acting capacity under clause (ii) or (iii) of subparagraph (B), or under subparagraph (C), with respect to only 1 Inspector General position at any given time.

(E) If the President makes a direction under subparagraph (B)(iii), during the 30-day period preceding the date on which the direction of the President takes effect, the functions and duties of the position of the Inspector General shall be performed by—

- (i) the first assistant to the position of Inspector General; or
- (ii) the individual performing those functions and duties temporarily in an acting capacity, as of the date on which the President issues that direction, if that individual is an individual other than the first assistant to the position of Inspector General.

(d) ASSISTANT INSPECTORS GENERAL.—

Subject to the policies of the Director of National Intelligence, the Inspector General of the Intelligence Community shall—

- (1) appoint an Assistant Inspector General for Audit who shall have the responsibility for supervising the performance of auditing activities relating to programs and activities within the responsibility and authority of the Director;
- (2) appoint an Assistant Inspector General for Investigations who shall have the responsibility for supervising the performance of investigative activities relating to such programs and activities; and
- (3) appoint other Assistant Inspectors General that, in the judgment of the Inspector General, are necessary to carry out the duties of the Inspector General.

(e) DUTIES AND RESPONSIBILITIES.—It shall be the duty and responsibility of the Inspector General of the Intelligence Community—

- (1) to provide policy direction for, and to plan, conduct, supervise, and coordinate independently, the investigations, inspections, audits, and reviews relating to programs and activities within the responsibility and authority of the Director of National Intelligence;

(2) to keep the Director of National Intelligence fully and currently informed concerning violations of law and regulations, fraud, and other serious problems, abuses, and deficiencies relating to the programs and activities within the responsibility and authority of the Director, to recommend corrective action concerning such problems, and to report on the progress made in implementing such corrective action;

(3) to take due regard for the protection of intelligence sources and methods in the preparation of all reports issued by the Inspector General, and, to the extent consistent with the purpose and objective of such reports, take such measures as may be appropriate to minimize the disclosure of intelligence sources and methods described in such reports; and

(4) in the execution of the duties and responsibilities under this section, to comply with generally accepted government auditing.

(f) LIMITATIONS ON ACTIVITIES.—

(1) The Director of National Intelligence may prohibit the Inspector General of the Intelligence Community from initiating, carrying out, or completing any investigation, inspection, audit, or review if the Director determines that such prohibition is necessary to protect vital national security interests of the United States.

(2) Not later than seven days after the date on which the Director exercises the authority under paragraph (1), the Director shall submit to the congressional intelligence committees an appropriately classified statement of the reasons for the exercise of such authority.

(3) The Director shall advise the Inspector General at the time a statement under paragraph (2) is submitted, and, to the extent consistent with the protection of intelligence sources and methods, provide the Inspector General with a copy of such statement.

(4) The Inspector General may submit to the congressional intelligence committees any comments on the statement of which the Inspector General has notice under paragraph (3) that the Inspector General considers appropriate.

(g) AUTHORITIES.—

(1) The Inspector General of the Intelligence Community shall have direct and prompt access to the Director of National Intelligence when necessary for any purpose pertaining to the performance of the duties of the Inspector General.

(2)(A) The Inspector General shall, subject to the limitations in subsection (f), make such investigations and reports relating to the administration of the programs and activities within the authorities and responsibilities of the Director as are, in the judgment of the Inspector General, necessary or desirable.

(B) The Inspector General shall have access to any employee, or any employee of a contractor, of any element of the intelligence community needed for the performance of the duties of the Inspector General.

(C) The Inspector General shall have direct access to all records, reports, audits, reviews, documents, papers, recommendations, or other materials that relate to the programs and activities with respect to which the Inspector General has responsibilities under this section.

(D) The level of classification or compartmentation of information shall not, in and of itself, provide a sufficient rationale for denying the Inspector General access to any materials under subparagraph (C).

(E) The Director, or on the recommendation of the Director, another appropriate official of the intelligence community, shall take appropriate administrative actions against an employee, or an employee of a contractor, of an element of the intelligence community that fails to cooperate with the Inspector General. Such administrative action may include loss of employment or the termination of an existing contractual relationship.

(3) The Inspector General is authorized to receive and investigate, pursuant to subsection (h), complaints or information from any person concerning the existence of an activity within the authorities and responsibilities of the Director of National Intelligence constituting a violation of laws, rules, or regulations, or mismanagement, gross waste of funds, abuse of authority, or a substantial and specific danger to the public health and safety. Once such complaint or information has been received from an employee of the intelligence community—

(A) the Inspector General shall not disclose the identity of the employee without the consent of the employee, unless the Inspector General determines that such disclosure is unavoidable during the course of the investigation or the disclosure is made to an official of the Department of Justice responsible for determining whether a prosecution should be undertaken, and this provision shall qualify as a withholding statute pursuant to subsection (b)(3) of section 552 of title 5, United States Code (commonly known as the “Freedom of Information Act”); and

(B) no action constituting a reprisal, or threat of reprisal, for making such complaint or disclosing such information to the Inspector General may be taken by any employee in a position to take such actions, unless the complaint was made or the

information was disclosed with the knowledge that it was false or with willful disregard for its truth or falsity.

(4) The Inspector General shall have the authority to administer to or take from any person an oath, affirmation, or affidavit, whenever necessary in the performance of the duties of the Inspector General, which oath, affirmation, or affidavit when administered or taken by or before an employee of the Office of the Inspector General of the Intelligence Community designated by the Inspector General shall have the same force and effect as if administered or taken by, or before, an officer having a seal.

(5)(A) Except as provided in subparagraph (B), the Inspector General is authorized to require by subpoena the production of all information, documents, reports, answers, records, accounts, papers, and other data in any medium (including electronically stored information, as well as any tangible thing) and documentary evidence necessary in the performance of the duties and responsibilities of the Inspector General.

(B) In the case of departments, agencies, and other elements of the United States Government, the Inspector General shall obtain information, documents, reports, answers, records, accounts, papers, and other data and evidence for the purpose specified in subparagraph (A) using procedures other than by subpoenas.

(C) The Inspector General may not issue a subpoena for, or on behalf of, any component of the Office of the Director of National Intelligence or any element of the intelligence community, including the Office of the Director of National Intelligence.

(D) In the case of contumacy or refusal to obey a subpoena issued under this paragraph, the subpoena shall be enforceable by order of any appropriate district court of the United States.

(6) The Inspector General may obtain services as authorized by section 3109 of title 5, United States Code, at rates for individuals not to exceed the daily equivalent of the maximum annual rate of basic pay payable for grade GS-15 of the General Schedule under section 5332 of title 5, United States Code.

(7) The Inspector General may, to the extent and in such amounts as may be provided in appropriations, enter into contracts and other arrangements for audits, studies, analyses, and other services with public agencies and with private persons, and to make such payments as may be necessary to carry out the provisions of this section.

(h) COORDINATION AMONG INSPECTORS GENERAL.—

(1)(A) In the event of a matter within the jurisdiction of the Inspector General of the Intelligence Community that may be subject to an

investigation, inspection, audit, or review by both the Inspector General of the Intelligence Community and an inspector general with oversight responsibility for an element of the intelligence community, the Inspector General of the Intelligence Community and such other inspector general shall expeditiously resolve the question of which inspector general shall conduct such investigation, inspection, audit, or review to avoid unnecessary duplication of the activities of the inspectors general.

(B) In attempting to resolve a question under subparagraph (A), the inspectors general concerned may request the assistance of the Intelligence Community Inspectors General Forum established under paragraph (2). In the event of a dispute between an inspector general within a department or agency of the United States Government and the Inspector General of the Intelligence Community that has not been resolved with the assistance of such Forum, the inspectors general shall submit the question to the Director of National Intelligence and the head of the affected department or agency for resolution.

(2)(A) There is established the Intelligence Community Inspectors General Forum, which shall consist of all statutory or administrative inspectors general with oversight responsibility for an element of the intelligence community.

(B) The Inspector General of the Intelligence Community shall serve as the Chair of the Forum established under subparagraph (A). The Forum shall have no administrative authority over any inspector general, but shall serve as a mechanism for informing its members of the work of individual members of the Forum that may be of common interest and discussing questions about jurisdiction or access to employees, employees of contract personnel, records, audits, reviews, documents, recommendations, or other materials that may involve or be of assistance to more than one of its members.

(3) The inspector general conducting an investigation, inspection, audit, or review covered by paragraph (1) shall submit the results of such investigation, inspection, audit, or review to any other inspector general, including the Inspector General of the Intelligence Community, with jurisdiction to conduct such investigation, inspection, audit, or review who did not conduct such investigation, inspection, audit, or review.

(i) COUNSEL TO THE INSPECTOR GENERAL.—

(1) The Inspector General of the Intelligence Community shall—

(A) appoint a Counsel to the Inspector General who shall report to the Inspector General; or

(B) obtain the services of a counsel appointed by and directly reporting to another inspector general or the Council of the Inspectors General on Integrity and Efficiency on a reimbursable basis.

(2) The counsel appointed or obtained under paragraph (1) shall perform such functions as the Inspector General may prescribe.

(j) STAFF AND OTHER SUPPORT.—

(1) The Director of National Intelligence shall provide the Inspector General of the Intelligence Community with appropriate and adequate office space at central and field office locations, together with such equipment, office supplies, maintenance services, and communications facilities and services as may be necessary for the operation of such offices.

(2)(A) Subject to applicable law and the policies of the Director of National Intelligence, the Inspector General shall select, appoint, and employ such officers and employees as may be necessary to carry out the functions, powers, and duties of the Inspector General. The Inspector General shall ensure that any officer or employee so selected, appointed, or employed has security clearances appropriate for the assigned duties of such officer or employee.

(B) In making selections under subparagraph (A), the Inspector General shall ensure that such officers and employees have the requisite training and experience to enable the Inspector General to carry out the duties of the Inspector General effectively.

(C) In meeting the requirements of this paragraph, the Inspector General shall create within the Office of the Inspector General of the Intelligence Community a career cadre of sufficient size to provide appropriate continuity and objectivity needed for the effective performance of the duties of the Inspector General.

(3) Consistent with budgetary and personnel resources allocated by the Director of National Intelligence, the Inspector General has final approval of—

(A) the selection of internal and external candidates for employment with the Office of the Inspector General; and

(B) all other personnel decisions concerning personnel permanently assigned to the Office of the Inspector General, including selection and appointment to the Senior Intelligence Service, but excluding all security-based determinations that are not within the authority of a head of a component of the Office of the Director of National Intelligence.

(4)(A) Subject to the concurrence of the Director of National Intelligence, the Inspector General may request such information or

assistance as may be necessary for carrying out the duties and responsibilities of the Inspector General from any Federal, State (as defined in section 805), or local governmental agency or unit thereof.

(B) Upon request of the Inspector General for information or assistance from a department, agency, or element of the Federal Government under subparagraph (A), the head of the department, agency, or element concerned shall, insofar as is practicable and not in contravention of any existing statutory restriction or regulation of the department, agency, or element, furnish to the Inspector General, such information or assistance.

(C) The Inspector General of the Intelligence Community may, upon reasonable notice to the head of any element of the intelligence community and in coordination with that element's inspector general pursuant to subsection (h), conduct, as authorized by this section, an investigation, inspection, audit, or review of such element and may enter into any place occupied by such element for purposes of the performance of the duties of the Inspector General.

(k) REPORTS.—

(1)(A) The Inspector General of the Intelligence Community shall, not later than October 31 and April 30 of each year, prepare and submit to the Director of National Intelligence a classified, and, as appropriate, unclassified semiannual report summarizing the activities of the Office of the Inspector General of the Intelligence Community during the immediately preceding 6-month period ending September 30 and March 31, respectively. The Inspector General of the Intelligence Community shall provide any portion of the report involving a component of a department of the United States Government to the head of that department simultaneously with submission of the report to the Director of National Intelligence.

(B) Each report under this paragraph shall include, at a minimum, the following:

(i) A list of the title or subject of each investigation, inspection, audit, or review conducted during the period covered by such report.

(ii) A description of significant problems, abuses, and deficiencies relating to the administration of programs and activities of the intelligence community within the responsibility and authority of the Director of National Intelligence, and in the relationships between elements of the intelligence community, identified by the

Inspector General during the period covered by such report.

(iii) A description of the recommendations for corrective action made by the Inspector General during the period covered by such report with respect to significant problems, abuses, or deficiencies identified in clause (ii).

(iv) A statement of whether or not corrective action has been completed on each significant recommendation described in previous semiannual reports, and, in a case where corrective action has been completed, a description of such corrective action.

(v) A certification of whether or not the Inspector General has had full and direct access to all information relevant to the performance of the functions of the Inspector General.

(vi) A description of the exercise of the subpoena authority under subsection (g)(5) by the Inspector General during the period covered by such report.

(vii) Such recommendations as the Inspector General considers appropriate for legislation to promote economy, efficiency, and effectiveness in the administration and implementation of programs and activities within the responsibility and authority of the Director of National Intelligence, and to detect and eliminate fraud and abuse in such programs and activities.

(C) Not later than 30 days after the date of receipt of a report under subparagraph (A), the Director shall transmit the report to the congressional intelligence committees together with any comments the Director considers appropriate. The Director shall transmit to the committees of the Senate and of the House of Representatives with jurisdiction over a department of the United States Government any portion of the report involving a component of such department simultaneously with submission of the report to the congressional intelligence committees.

(2)(A) The Inspector General shall report immediately to the Director whenever the Inspector General becomes aware of particularly serious or flagrant problems, abuses, or deficiencies relating to programs and activities within the responsibility and authority of the Director of National Intelligence.

(B) The Director shall transmit to the congressional intelligence

committees each report under subparagraph (A) within 7 calendar days of receipt of such report, together with such comments as the Director considers appropriate. The Director shall transmit to the committees of the Senate and of the House of Representatives with jurisdiction over a department of the United States Government any portion of each report under subparagraph (A) that involves a problem, abuse, or deficiency related to a component of such department simultaneously with transmission of the report to the congressional intelligence committees.

(3)(A) In the event that—

- (i) the Inspector General is unable to resolve any differences with the Director affecting the execution of the duties or responsibilities of the Inspector General;
- (ii) an investigation, inspection, audit, or review carried out by the Inspector General focuses on any current or former intelligence community official who—
 - (I) holds or held a position in an element of the intelligence community that is subject to appointment by the President, whether or not by and with the advice and consent of the Senate, including such a position held on an acting basis;
 - (II) holds or held a position in an element of the intelligence community, including a position held on an acting basis, that is appointed by the Director of National Intelligence; or
 - (III) holds or held a position as head of an element of the intelligence community or a position covered by subsection (b) or (c) of section 106;
- (iii) a matter requires a report by the Inspector General to the Department of Justice on possible criminal conduct by a current or former official described in clause (ii);
- (iv) the Inspector General receives notice from the Department of Justice declining or approving prosecution of possible criminal conduct of any current or former official described in clause (ii); or
- (v) the Inspector General, after exhausting all possible alternatives, is unable to obtain significant documentary information in the course of an investigation, inspection,

audit, or review, the Inspector General shall immediately notify, and submit a report to, the congressional intelligence committees on such matter.

(B) The Inspector General shall submit to the committees of the Senate and of the House of Representatives with jurisdiction over a department of the United States Government any portion of each report under subparagraph (A) that involves an investigation, inspection, audit, or review carried out by the Inspector General focused on any current or former official of a component of such department simultaneously with submission of the report to the congressional intelligence committees.

(4) The Director shall submit to the congressional intelligence committees any report or findings and recommendations of an investigation, inspection, audit, or review conducted by the office which has been requested by the Chairman or Vice Chairman or ranking minority member of either committee.

(5)(A) An employee of an element of the intelligence community, an employee assigned or detailed to an element of the intelligence community, or an employee of a contractor to the intelligence community who intends to report to Congress a complaint or information with respect to an urgent concern may report such complaint or information to the Inspector General.

(B) Not later than the end of the 14-calendar-day period beginning on the date of receipt from an employee of a complaint or information under subparagraph (A), the Inspector General shall determine whether the complaint or information appears credible. Upon making such a determination, the Inspector General shall transmit to the Director a notice of that determination, together with the complaint or information.

(C) Upon receipt of a transmittal from the Inspector General under subparagraph (B), the Director shall, within 7 calendar days of such receipt, forward such transmittal to the congressional intelligence committees, together with any comments the Director considers appropriate.

(D)(i) If the Inspector General does not find credible under subparagraph (B) a complaint or information submitted under subparagraph (A), or does not transmit the complaint or information to the Director in accurate form under subparagraph (B), the employee (subject to clause (ii)) may submit the complaint or information to Congress by contacting either or both of the congressional intelligence committees directly.

(ii) An employee may contact the congressional intelligence committees directly as described in clause

(i) only if the employee—

(I) before making such a contact, furnishes to the Director, through the Inspector General, a statement of the employee's complaint or information and notice of the employee's intent to contact the congressional intelligence committees directly; and

(II) obtains and follows from the Director, through the Inspector General, direction on how to contact the congressional intelligence committees in accordance with appropriate security practices.

(iii) A member or employee of one of the congressional intelligence committees who receives a complaint or information under this subparagraph does so in that member or employee's official capacity as a member or employee of such committee.

(E) The Inspector General shall notify an employee who reports a complaint or information to the Inspector General under this paragraph of each action taken under this paragraph with respect to the complaint or information. Such notice shall be provided not later than 3 days after any such action is taken.

(F) An action taken by the Director or the Inspector General under this paragraph shall not be subject to judicial review.

(G)(i) In this paragraph, the term "urgent concern" means any of the following:

(I) A serious or flagrant problem, abuse, violation of law or Executive order, or deficiency relating to the funding, administration, or operation of an intelligence activity of the Federal Government that is—

(aa) a matter of national security; and

(bb) not a difference of opinion concerning public policy matters.

(II) A false statement to Congress, or a willful withholding from Congress, on an issue of material fact relating to the funding, administration, or operation of an intelligence activity.

(III) An action, including a personnel action described in section 2302(a)(2)(A) of title 5, United States Code, constituting reprisal or threat of reprisal prohibited under subsection (g)(3)(B) of this section in response to an employee's reporting an urgent concern in accordance with this paragraph.

(ii) Within the executive branch, the Inspector General shall have sole authority to determine whether any complaint or information reported to the Inspector General is a matter of urgent concern under this paragraph.

(H) Nothing in this section shall be construed to limit the protections afforded to an employee under section 17(d) of the Central Intelligence Agency Act of 1949 [50 U.S.C. 3517(d)] or section 416 of title 5, United States Code.

(I) An individual who has submitted a complaint or information to the Inspector General under this section may notify any member of either of the congressional intelligence committees, or a staff member of either of such committees, of the fact that such individual has made a submission to the Inspector General, and of the date on which such submission was made.

(6) In accordance with section 535 of title 28, United States Code, the Inspector General shall expeditiously report to the Attorney General any information, allegation, or complaint received by the Inspector General relating to violations of Federal criminal law that involves a program or operation of an element of the intelligence community, or in the relationships between the elements of the intelligence community, consistent with such guidelines as may be issued by the Attorney General pursuant to subsection (b)(2) of such section. A copy of each such report shall be furnished to the Director.

(l) CONSTRUCTION OF DUTIES REGARDING ELEMENTS OF INTELLIGENCE COMMUNITY.—Except as resolved pursuant to subsection (h), the performance by the Inspector General of the Intelligence Community of any duty, responsibility, or function regarding an element of the intelligence community shall not be construed to modify or affect the duties and responsibilities of any other inspector general having duties and responsibilities relating to such element.

(m) SEPARATE BUDGET ACCOUNT.—The Director of National Intelligence shall, in accordance with procedures issued by the Director in consultation with the congressional intelligence committees, include in the National Intelligence Program budget a separate account for the Office of the Inspector General of the Intelligence Community.

(n) BUDGET.—

- (1) For each fiscal year, the Inspector General of the Intelligence Community shall transmit a budget estimate and request to the Director of National Intelligence that specifies for such fiscal year—
 - (A) the aggregate amount requested for the operations of the Inspector General;
 - (B) the amount requested for all training requirements of the Inspector General, including a certification from the Inspector General that the amount requested is sufficient to fund all training requirements for the Office of the Inspector General; and
 - (C) the amount requested to support the Council of the Inspectors General on Integrity and Efficiency, including a justification for such amount.
- (2) In transmitting a proposed budget to the President for a fiscal year, the Director of National Intelligence shall include for such fiscal year—
 - (A) the aggregate amount requested for the Inspector General of the Intelligence Community;
 - (B) the amount requested for Inspector General training;
 - (C) the amount requested to support the Council of the Inspectors General on Integrity and Efficiency; and
 - (D) the comments of the Inspector General, if any, with respect to such proposed budget.
- (3) The Director of National Intelligence shall submit to the congressional intelligence committees, the Committee on Appropriations of the Senate, and the Committee on Appropriations of the House of Representatives for each fiscal year—
 - (A) a separate statement of the budget estimate transmitted pursuant to paragraph (1);
 - (B) the amount requested by the Director for the Inspector General pursuant to paragraph (2)(A);
 - (C) the amount requested by the Director for the training of personnel of the Office of the Inspector General pursuant to paragraph (2)(B);
 - (D) the amount requested by the Director for support for the Council of the Inspectors General on Integrity and Efficiency pursuant to paragraph (2)(C); and
 - (E) the comments of the Inspector General under paragraph (2)(D), if any, on the amounts requested pursuant to paragraph (2), including whether such amounts would substantially inhibit the Inspector General from performing the duties of the Office of the Inspector General.

(o) INFORMATION ON WEBSITE.—

(1) The Director of National Intelligence shall establish and maintain on the homepage of the publicly accessible website of the Office of the Director of National Intelligence information relating to the Office of the Inspector General of the Intelligence Community including methods to contact the Inspector General.

(2) The information referred to in paragraph (1) shall be obvious and facilitate accessibility to the information related to the Office of the Inspector General of the Intelligence Community.

CHIEF FINANCIAL OFFICER OF THE INTELLIGENCE COMMUNITY

SEC. 103I. [50 U.S.C. § 3034]

(a) CHIEF FINANCIAL OFFICER OF THE INTELLIGENCE COMMUNITY.—To assist the Director of National Intelligence in carrying out the responsibilities of the Director under this Act and other applicable provisions of law, there is within the Office of the Director of National Intelligence a Chief Financial Officer of the Intelligence Community who shall be appointed by the Director. The Chief Financial Officer shall report directly to the Director of National Intelligence.

(b) DUTIES AND RESPONSIBILITIES.—Subject to the direction of the Director of National Intelligence, the Chief Financial Officer of the Intelligence Community shall—

(1) serve as the principal advisor to the Director of National Intelligence and the Principal Deputy Director of National Intelligence on the management and allocation of intelligence community budgetary resources;

(2) participate in overseeing a comprehensive and integrated strategic process for resource management within the intelligence community;

(3) ensure that the strategic plan of the Director of National Intelligence—

(A) is based on budgetary constraints as specified in the Future Year Intelligence Plans and Long-term Budget Projections required under section 506G; and

(B) contains specific goals and objectives to support a performance-based budget;

(4) prior to the obligation or expenditure of funds for the acquisition of any major system pursuant to a Milestone A or Milestone B decision, receive verification from appropriate authorities that the national requirements for meeting the strategic plan of the Director have been established, and that such requirements are prioritized based on budgetary constraints as specified in the Future Year Intelligence Plans

and the Long-term Budget Projections for such major system required under section 506G;

(5) ensure that the collection architectures of the Director are based on budgetary constraints as specified in the Future Year Intelligence Plans and the Long-term Budget Projections required under section 506G;

(6) coordinate or approve representations made to Congress by the intelligence community regarding National Intelligence Program budgetary resources;

(7) participate in key mission requirements, acquisitions, or architectural boards formed within or by the Office of the Director of National Intelligence; and

(8) perform such other duties as may be prescribed by the Director of National Intelligence.

(c) **OTHER LAW.**—The Chief Financial Officer of the Intelligence Community shall serve as the Chief Financial Officer of the intelligence community and, to the extent applicable, shall have the duties, responsibilities, and authorities specified in chapter 9 of title 31, United States Code.

(d) **PROHIBITION ON SIMULTANEOUS SERVICE AS OTHER CHIEF FINANCIAL OFFICER.**—An individual serving in the position of Chief Financial Officer of the Intelligence Community may not, while so serving, serve as the chief financial officer of any other department or agency, or component thereof, of the United States Government.

(e) **DEFINITIONS.**—In this section:

(1) The term “major system” has the meaning given that term in section 506A(e).

(2) The term “Milestone A” has the meaning given that term in section 506G(f).

(3) The term “Milestone B” has the meaning given that term in section 506C(e).

FUNCTIONAL MANAGERS FOR THE INTELLIGENCE COMMUNITY

SEC. 103J. [50 U.S.C. § 3034a]

(a) **FUNCTIONAL MANAGERS AUTHORIZED.**—The Director of National Intelligence may establish within the intelligence community one or more positions of manager of an intelligence function. Any position so established may be known as the “Functional Manager” of the intelligence function concerned.

(b) **PERSONNEL.**—The Director shall designate individuals to serve as manager of intelligence functions established under subsection (a) from among officers and employees of elements of the intelligence community.

(c) **DUTIES.**—Each manager of an intelligence function established under subsection (a) shall have the duties as follows:

- (1) To act as principal advisor to the Director on the intelligence function.
- (2) To carry out such other responsibilities with respect to the intelligence function as the Director may specify for purposes of this section.

INTELLIGENCE COMMUNITY CHIEF DATA OFFICER

SEC. 103K. [50 U.S.C. § 3034b]

(a) **INTELLIGENCE COMMUNITY CHIEF DATA OFFICER.** —There is an Intelligence Community Chief Data Officer within the Office of the Director of National Intelligence who shall be appointed by the Director of National Intelligence.

(b) **REQUIREMENT RELATING TO APPOINTMENT.** —An individual appointed as the Intelligence Community Chief Data Officer shall have a professional background and experience appropriate for the duties of the Intelligence Community Chief Data Officer. In making such appointment, the Director of National Intelligence may give preference to an individual with experience outside of the United States Government.

(c) **DUTIES.** —The Intelligence Community Chief Data Officer shall—

- (1) act as the chief representative of the Director of National Intelligence for data issues within the intelligence community;
- (2) coordinate, to the extent practicable and advisable, with the Chief Data Officer of the Department of Defense to ensure consistent data policies, standards, and procedures between the intelligence community and the Department of Defense;
- (3) assist the Director of National Intelligence regarding data elements of the budget of the Office of the Director of National Intelligence; and
- (4) perform other such duties relating to data as may be prescribed by the Director of National Intelligence or specified in law.

INTELLIGENCE COMMUNITY INNOVATION UNIT

SEC. 103L. [50 U.S.C. § 3043(c)]

(a) **DEFINITIONS.**—In this section:

(1) **Emerging technology.**—the term ‘emerging technology’ has the meaning given that term in section 6701 of the Intelligence Authorization Act for Fiscal Year 2023 (Public Law 117–263; 50 U.S.C. 3024 note).

(2) **UNIT.**—The term ‘Unit’ means the Intelligence Community Innovation Unit.

(b) **PLAN FOR IMPLEMENTATION OF INTELLIGENCE COMMUNITY INNOVATION UNIT.**—

(1) **PLAN REQUIRED.**—Not later than 180 days after the date of the enactment of the Intelligence Authorization Act for Fiscal Year 2024, the

Director of National Intelligence shall develop a plan for how to implement the Intelligence Community Innovation Unit within the intelligence community.

(2) **MATTERS COVERED.**—The plan developed pursuant to paragraph (1) shall cover how the Unit will—

(A) benefit heads of the elements of the intelligence community in identifying commercial emerging technologies and associated capabilities to address critical mission needs of elements of the intelligence community;

(B) provide to the heads of the elements of the intelligence community seeking to field commercial emerging technologies technical expertise with respect to such technologies.

(C) facilitate the transition of potential prototypes and solutions to critical mission needs of the intelligence community from research and prototype projects to production; and

(D) serve as a liaison between the intelligence community and the private sector, in which capacity such liaison shall focus on small- and medium-sized companies and other organizations that do not have significant experience engaging with the intelligence community.

(3) **REQUIREMENTS.**—The plan developed pursuant to paragraph (1) shall—

(A) plan for not more than 50 full-time equivalent personnel; and

(B) include an assessment as to how the establishment of the Unit would benefit the identification and evaluation of commercial emerging technologies for prototyping and potential adoption by the intelligence community to fulfill critical mission needs.

(4) **SUBMISSION TO CONGRESS.**—Upon completing development of the plan pursuant to paragraph (1), the Director shall—

(A) submit to the congressional intelligence committees, the Subcommittee on Defense of the Committee on Appropriations of the Senate, and the Subcommittee on Defense of the Committee on Appropriations of the House of Representatives a copy of the plan; and

(B) provide such committees and subcommittees a briefing on the plan.

(c) **ESTABLISHMENT.**—To the extent and in such amounts as specifically provided in advance in appropriations Acts for the purposes detailed in this section, not later than 180 days after the date on which the Director of National Intelligence submits the plan pursuant to subsection (b)(4)(A), the Director of National Intelligence shall establish the Unit within the Office of the Director of National Intelligence.

NATIONAL SECURITY ACT OF 1947

(d) LIMITATION.—The Unit shall not abrogate or otherwise constrain any element of the intelligence community from conducting authorized activities.

(e) DIRECTOR OF THE INTELLIGENCE COMMUNITY INNOVATION UNIT.—

(1) APPOINTMENT; REPORTING.—The head of the Unit is the Director of the Intelligence Community Innovation Unit, who shall be appointed by the Director of National Intelligence and shall report directly to the Director of National Intelligence.

(2) QUALIFICATIONS.—In selecting an individual for appointment as the Director of the Intelligence Community Innovation Unit, the Director of National Intelligence shall give preference to individuals who the Director of National Intelligence determines have—

(A) significant relevant experience involving commercial emerging technology within the private sector; and

(B) a demonstrated history of fostering the adoption of commercial emerging technologies by the United States Government or the private sector.

(f) STAFF.—

(1) IN GENERAL.—In addition to the Director of the Intelligence Community Innovation Unit, the Unit shall be composed of not more than 50 full-time equivalent positions.

(2) STAFF WITH CERTAIN EXPERTISE.—The Director of National Intelligence shall ensure that there is a sufficient number of staff of the Unit, as determined by the Director, with expertise in—

(A) other transaction authorities and nontraditional and rapid acquisition pathways for emerging technology;

(B) engaging and evaluating small- and medium-sized emerging technology companies;

(C) the mission needs of the intelligence community; and

(D) such other skills or experiences as the Director determines necessary.

(g) AUTHORITY RELATING TO DETAILEES.—Upon request of the Unit, each head of an element of the intelligence community may detail to the Unit any of the personnel of that element to assist in carrying out the duties under subsection (b) on a reimbursable or a nonreimbursable basis.

(h) ENSURING TRANSITION FROM PROTOTYPING TO PRODUCTION.—The Director of the Intelligence Community Innovation Unit shall transition research and prototype projects to products in a production stage upon identifying a demonstrated critical mission need of one or more elements of the intelligence community and a potential mission partner likely to field and further fund upon maturation, including by designating projects as Emerging Technology Transition Projects under the pilot program required by section 6713 of the

NATIONAL SECURITY ACT OF 1947

Intelligence Authorization Act for Fiscal Year 2023 (Public Law 117–263; 50 U.S.C. 3024 note).

(i) **ENCOURAGEMENT OF USE BY ELEMENTS.**—The Director of National Intelligence shall take such steps as may be necessary to encourage the use of the Unit by the heads of the other elements of the intelligence community.

(j) **RULES OF CONSTRUCTION.**—

(1) **NO PREFERENTIAL TREATMENT FOR PRIVATE SECTOR.**— Nothing in this section shall be construed to require any element of the intelligence community to provide preferential treatment for any private sector entity with regard to procurement of technology construed as restricting or preempting any activities of the intelligence community.

(2) **NO ADDITIONAL AUTHORITY.**—The Unit established pursuant to subsection (c) will be limited to the existing authorities possessed by the Director of National Intelligence.

(k) **SUNSET.**—The authorities and requirements of this section shall terminate on the date that is 5 years after the date of the establishment of the Unit.

CENTRAL INTELLIGENCE AGENCY

SEC. 104. [50 U.S.C. § 3035]

(a) **CENTRAL INTELLIGENCE AGENCY.**—There is a Central Intelligence Agency.

(b) **FUNCTION.**—The function of the Central Intelligence Agency is to assist the Director of the Central Intelligence Agency in carrying out the responsibilities specified in section 104A(c).

DIRECTOR OF THE CENTRAL INTELLIGENCE AGENCY

SEC. 104A. [50 U.S.C. § 3036]

(a) **DIRECTOR OF CENTRAL INTELLIGENCE AGENCY.**—There is a Director of the Central Intelligence Agency who shall be appointed by the President, by and with the advice and consent of the Senate.

(b) **SUPERVISION.**—The Director of the Central Intelligence Agency shall report to the Director of National Intelligence regarding the activities of the Central Intelligence Agency.

(c) **DUTIES.**—The Director of the Central Intelligence Agency shall—

- (1) serve as the head of the Central Intelligence Agency; and
- (2) carry out the responsibilities specified in subsection (d).

(d) **RESPONSIBILITIES.**—The Director of the Central Intelligence Agency shall—

- (1) collect intelligence through human sources and by other appropriate means, except that the Director of the Central Intelligence Agency shall have no police, subpoena, or law enforcement powers or internal security functions;

- (2) correlate and evaluate intelligence related to the national security and provide appropriate dissemination of such intelligence;
- (3) provide overall direction for and coordination of the collection of national intelligence outside the United States through human sources by elements of the intelligence community authorized to undertake such collection and, in coordination with other departments, agencies, or elements of the United States Government which are authorized to undertake such collection, ensure that the most effective use is made of resources and that appropriate account is taken of the risks to the United States and those involved in such collection; and
- (4) perform such other functions and duties related to intelligence affecting the national security as the President or the Director of National Intelligence may direct.

(e) **TERMINATION OF EMPLOYMENT OF CIA EMPLOYEES.**—

(1) Notwithstanding the provisions of any other law, the Director of the Central Intelligence Agency may, in the discretion of the Director, terminate the employment of any officer or employee of the Central Intelligence Agency whenever the Director deems the termination of employment of such officer or employee necessary or advisable in the interests of the United States.

(2) Any termination of employment of an officer or employee under paragraph (1) shall not affect the right of the officer or employee to seek or accept employment in any other department, agency, or element of the United States Government if declared eligible for such employment by the Office of Personnel Management.

(f) **COORDINATION WITH FOREIGN GOVERNMENTS.**—Under the direction of the Director of National Intelligence and in a manner consistent with section 207 of the Foreign Service Act of 1980 (22 U.S.C. 3927), the Director of the Central Intelligence Agency shall coordinate the relationships between elements of the intelligence community and the intelligence or security services of foreign governments or international organizations on all matters involving intelligence related to the national security or involving intelligence acquired through clandestine means.

DEPUTY DIRECTOR OF THE CENTRAL INTELLIGENCE AGENCY

SEC. 104B. [50 U.S.C. § 3037]

(a) **DEPUTY DIRECTOR OF THE CENTRAL INTELLIGENCE AGENCY.**—There is a Deputy Director of the Central Intelligence Agency who shall be appointed by the President.

(b) **DUTIES.**—The Deputy Director of the Central Intelligence Agency shall—

- (1) assist the Director of the Central Intelligence Agency in carrying out the duties and responsibilities of the Director of the Central Intelligence Agency; and
- (2) during the absence or disability of the Director of the Central Intelligence Agency, or during a vacancy in the position of Director of the Central Intelligence Agency, act for and exercise the powers of the Director of the Central Intelligence Agency.

**RESPONSIBILITIES OF THE SECRETARY OF DEFENSE
PERTAINING TO THE NATIONAL INTELLIGENCE PROGRAM**

SEC. 105. [50 U.S.C. § 3038]

(a) IN GENERAL.—Consistent with the sections 102 and 102A, the Secretary of Defense, in consultation with the Director of National Intelligence, shall—

- (1) ensure that the budgets of the elements of the intelligence community within the Department of Defense are adequate to satisfy the overall intelligence needs of the Department of Defense, including the needs of the Chairman of the Joint Chiefs of Staff and the commanders of the unified and specified commands and, wherever such elements are performing governmentwide functions, the needs of other departments and agencies;
- (2) ensure appropriate implementation of the policies and resource decisions of the Director by elements of the Department of Defense within the National Intelligence Program;
- (3) ensure that the tactical intelligence activities of the Department of Defense complement and are compatible with intelligence activities under the National Intelligence Program;
- (4) ensure that the elements of the intelligence community within the Department of Defense are responsive and timely with respect to satisfying the needs of operational military forces;
- (5) eliminate waste and unnecessary duplication among the intelligence activities of the Department of Defense; and
- (6) ensure that intelligence activities of the Department of Defense are conducted jointly where appropriate.

(b) RESPONSIBILITY FOR THE PERFORMANCE OF SPECIFIC FUNCTIONS.—

Consistent with sections 102 and 102A of this Act, the Secretary of Defense shall ensure—

- (1) through the National Security Agency (except as otherwise directed by the President or the National Security Council), the continued operation of an effective unified organization for the conduct of signals intelligence activities and shall ensure that the product is disseminated in a timely manner to authorized recipients;

(2) through the National Geospatial-Intelligence Agency (except as otherwise directed by the President or the National Security Council), with appropriate representation from the intelligence community, the continued operation of an effective unified organization within the Department of Defense—

- (A) for carrying out tasking of imagery collection;
- (B) for the coordination of imagery processing and exploitation activities;
- (C) for ensuring the dissemination of imagery in a timely manner to authorized recipients; and
- (D) notwithstanding any other provision of law, for—
 - (i) prescribing technical architecture and standards related to imagery intelligence and geospatial information and ensuring compliance with such architecture and standards; and
 - (ii) developing and fielding systems of common concern related to imagery intelligence and geospatial information;

(3) through the National Reconnaissance Office (except as otherwise directed by the President or the National Security Council), the continued operation of an effective unified organization for the research and development, acquisition, and operation of overhead reconnaissance systems necessary to satisfy the requirements of all elements of the intelligence community;

(4) through the Defense Intelligence Agency (except as otherwise directed by the President or the National Security Council), the continued operation of an effective unified system within the Department of Defense for the production of timely, objective military and military-related intelligence, based upon all sources available to the intelligence community, and shall ensure the appropriate dissemination of such intelligence to authorized recipients;

(5) through the Defense Intelligence Agency (except as otherwise directed by the President or the National Security Council), effective management of Department of Defense human intelligence and counterintelligence activities, including defense attaches; and

(6) that the military departments maintain sufficient capabilities to collect and produce intelligence to meet—

- (A) the requirements of the Director of National Intelligence;
- (B) the requirements of the Secretary of Defense or the Chairman of the Joint Chiefs of Staff;
- (C) the requirements of the unified and specified combatant commands and of joint operations; and

(D) the specialized requirements of the military departments for intelligence necessary to support tactical commanders, military planners, the research and development process, the acquisition of military equipment, and training and doctrine.

(c) EXPENDITURE OF FUNDS BY THE DEFENSE INTELLIGENCE AGENCY.—

(1) Subject to paragraphs (2) and (3), the Director of the Defense Intelligence Agency may expend amounts made available to the Director under the National Intelligence Program for human intelligence and counterintelligence activities for objects of a confidential, extraordinary, or emergency nature, without regard to the provisions of law or regulation relating to the expenditure of Government funds.

(2) The Director of the Defense Intelligence Agency may not expend more than five percent of the amounts made available to the Director under the National Intelligence Program for human intelligence and counterintelligence activities for a fiscal year for objects of a confidential, extraordinary, or emergency nature in accordance with paragraph (1) during such fiscal year unless—

(A) the Director notifies the congressional intelligence committees, the Committee on Armed Services of the Senate, and the Committee on Armed Services of the House of Representatives, of the intent to expend the amounts; and

(B) 30 days have elapsed from the date on which the Director notifies the congressional intelligence committees, the Committee on Armed Services of the Senate, and the Committee on Armed Services of the House of Representatives, in accordance with subparagraph (A).

(3) For each expenditure referred to in paragraph (1), the Director shall certify that such expenditure was made for an object of a confidential, extraordinary, or emergency nature.

(4) Not later than December 31 of each year, the Director of the Defense Intelligence Agency shall submit to the congressional intelligence committees, the Committee on Armed Services of the Senate, and the Committee on Armed Services of the House of Representatives, a report on any expenditures made during the preceding fiscal year in accordance with paragraph (1).

(d) USE OF ELEMENTS OF DEPARTMENT OF DEFENSE.—The Secretary of Defense, in carrying out the functions described in this section, may use such elements of the Department of Defense as may be appropriate for the execution of those functions, in addition to, or in lieu of, the elements identified in this section.

ASSISTANCE TO UNITED STATES LAW ENFORCEMENT AGENCIES

SEC. 105A. [50 U.S.C. § 3039]

(a) **AUTHORITY TO PROVIDE ASSISTANCE.**—Subject to subsection (b), elements of the intelligence community may, upon the request of a United States law enforcement agency, collect information outside the United States about individuals who are not United States persons. Such elements may collect such information notwithstanding that the law enforcement agency intends to use the information collected for purposes of a law enforcement investigation or counterintelligence investigation.

(b) **LIMITATION ON ASSISTANCE BY ELEMENTS OF DEPARTMENT OF DEFENSE.**—

(1) With respect to elements within the Department of Defense, the authority in subsection (a) applies only to the following:

- (A) The National Security Agency.
- (B) The National Reconnaissance Office.
- (C) The National Geospatial-Intelligence Agency.
- (D) The Defense Intelligence Agency.

(2) Assistance provided under this section by elements of the Department of Defense may not include the direct participation of a member of the Army, Navy, Air Force, or Marine Corps in an arrest or similar activity.

(3) Assistance may not be provided under this section by an element of the Department of Defense if the provision of such assistance will adversely affect the military preparedness of the United States.

(4) The Secretary of Defense shall prescribe regulations governing the exercise of authority under this section by elements of the Department of Defense, including regulations relating to the protection of sources and methods in the exercise of such authority.

(c) **DEFINITIONS.**—For purposes of subsection (a):

(1) The term “United States law enforcement agency” means any department or agency of the Federal Government that the Attorney General designates as law enforcement agency for purposes of this section.

(2) The term “United States person” means the following:

- (A) A United States citizen.
- (B) An alien known by the intelligence agency concerned to be a permanent resident alien.
- (C) An unincorporated association substantially composed of United States citizens or permanent resident aliens.
- (D) A corporation incorporated in the United States, except for a corporation directed and controlled by a foreign government or governments.

**DISCLOSURE OF FOREIGN INTELLIGENCE ACQUIRED
IN CRIMINAL INVESTIGATIONS; NOTICE OF CRIMINAL
INVESTIGATIONS OF FOREIGN INTELLIGENCE SOURCES**

SEC. 105B. [50 U.S.C. § 3040]

(a) DISCLOSURE OF FOREIGN INTELLIGENCE.—

(1) Except as otherwise provided by law and subject to paragraph (2), the Attorney General, or the head of any other department or agency of the Federal Government with law enforcement responsibilities, shall expeditiously disclose to the Director of National Intelligence, pursuant to guidelines developed by the Attorney General in consultation with the Director, foreign intelligence acquired by an element of the Department of Justice or an element of such department or agency, as the case may be, in the course of a criminal investigation.

(2) The Attorney General by regulation and in consultation with the Director may provide for exceptions to the applicability of paragraph (1) for one or more classes of foreign intelligence, or foreign intelligence with respect to one or more targets or matters, if the Attorney General determines that disclosure of such foreign intelligence under that paragraph would jeopardize an ongoing law enforcement investigation or impair other significant law enforcement interests.

(b) PROCEDURES FOR NOTICE OF CRIMINAL INVESTIGATIONS.—Not later than 180 days after the date of enactment of this section, the Attorney General, in consultation with the Director of National Intelligence, shall develop guidelines to ensure that after receipt of a report from an element of the intelligence community of activity of a foreign intelligence source or potential foreign intelligence source that may warrant investigation as criminal activity, the Attorney General provides notice to the Director, within a reasonable period of time, of his intention to commence, or decline to commence, a criminal investigation of such activity.

(c) PROCEDURES.—The Attorney General shall develop procedures for the administration of this section, including the disclosure of foreign intelligence by elements of the Department of Justice, and elements of other departments and agencies of the Federal Government, under subsection (a) and the provision of notice with respect to criminal investigations under subsection (b).

PROHIBITION ON COLLECTION AND MAINTENANCE OF INFORMATION OF UNITED STATES PERSONS BASED ON FIRST AMENDMENT-PROTECTED ACTIVITIES.

SEC. 105C [50 U.S.C. § 3040a]

No element of the intelligence community may collect or maintain information concerning a United States person (as defined in section 105A) solely for the purpose of monitoring an activity protected by the first amendment to the Constitution of the United States.

APPOINTMENT OF OFFICIALS RESPONSIBLE FOR INTELLIGENCE-RELATED ACTIVITIES

SEC. 106. [50 U.S.C. § 3041]

(a) RECOMMENDATION OF DNI IN CERTAIN APPOINTMENTS.—

(1) In the event of a vacancy in a position referred to in paragraph (2), the Director of National Intelligence shall recommend to the President an individual for nomination to fill the vacancy.

(2) Paragraph (1) applies to the following positions:

(A) The Principal Deputy Director of National Intelligence.

(B) The Director of the Central Intelligence Agency.

(b) CONCURRENCE OF DNI IN APPOINTMENTS TO POSITIONS IN THE INTELLIGENCE COMMUNITY.—

(1) In the event of a vacancy in a position referred to in paragraph (2), the head of the department or agency having jurisdiction over the position shall obtain the concurrence of the Director of National Intelligence before appointing an individual to fill the vacancy or recommending to the President an individual to be nominated to fill the vacancy. If the Director does not concur in the recommendation, the head of the department or agency concerned may not fill the vacancy or make the recommendation to the President (as the case may be). In the case in which the Director does not concur in such a recommendation, the Director and the head of the department or agency concerned may advise the President directly of the intention to withhold concurrence or to make a recommendation, as the case may be.

(2) Paragraph (1) applies to the following positions:

(A) The Director of the National Security Agency.

(B) The Director of the National Reconnaissance Office.

(C) The Director of the National Geospatial-Intelligence Agency.

(D) The Assistant Secretary of State for Intelligence and Research.

- (E) The Director of the Office of Intelligence and Counterintelligence of the Department of Energy.
- (F) The Assistant Secretary for Intelligence and Analysis of the Department of the Treasury.
- (G) The Executive Assistant Director for Intelligence of the Federal Bureau of Investigation or any successor to that position.
- (H) The Under Secretary of Homeland Security for Intelligence and Analysis.

(c) CONSULTATION WITH DNI IN CERTAIN POSITIONS.—

(1) In the event of a vacancy in a position referred to in paragraph (2), the head of the department or agency having jurisdiction over the position shall consult with the Director of National Intelligence before appointing an individual to fill the vacancy or recommending to the President an individual to be nominated to fill the vacancy.

(2) Paragraph (1) applies to the following positions:

- (A) The Director of the Defense Intelligence Agency.
- (B) The Assistant Commandant of the Coast Guard for Intelligence.
- (C) Assistant Attorney General designated as the Assistant Attorney General for National Security under section 507A of title 28, United States Code.

DIRECTOR OF THE NATIONAL RECONNAISSANCE OFFICE

SEC. 106A. [50 U.S.C. § 3041a]

- (a) IN GENERAL.—There is a Director of the National Reconnaissance Office.
- (b) APPOINTMENT.—The Director of the National Reconnaissance Office shall be appointed by the President, by and with the advice and consent of the Senate.
- (c) FUNCTIONS AND DUTIES.—The Director of the National Reconnaissance Office shall be the head of the National Reconnaissance Office and shall discharge such functions and duties as are provided by this Act or otherwise by law or executive order.
- (d) ADVISORY BOARD.—
 - (1) ESTABLISHMENT.—There is established in the National Reconnaissance Office an advisory board (in this section referred to as the “Board”).
 - (2) DUTIES.—The Board shall—
 - (A) study matters relating to the mission of the National Reconnaissance Office, including with respect to promoting innovation, competition, and resilience in space, overhead reconnaissance, acquisition, and other matters; and

(B) advise and report directly to the Director with respect to such matters.

(3) MEMBERS.—

(A) NUMBER AND APPOINTMENT.—

(i) IN GENERAL.—The Board shall be composed of five members appointed by the Director, in consultation with the Director of National Intelligence and the Secretary of Defense, from among individuals with demonstrated academic, government, business, or other expertise relevant to the mission and functions of the National Reconnaissance Office.

(ii) NOTIFICATION.—Not later than 30 days after the date on which the Director appoints a member to the Board, the Director shall notify the congressional intelligence committees and the congressional defense committees (as defined in section 101(a) of title 10, United States Code) of such appointment.

(B) TERMS.—Each member shall be appointed for a term of 2 years. Except as provided by subparagraph (C), a member may not serve more than three terms.

(C) VACANCY.—Any member appointed to fill a vacancy occurring before the expiration of the term for which the member's predecessor was appointed shall be appointed only for the remainder of that term. A member may serve after the expiration of that member's term until a successor has taken office.

(D) CHAIR.—The Board shall have a Chair, who shall be appointed by the Director from among the members.

(E) TRAVEL EXPENSES.—Each member shall receive travel expenses, including per diem in lieu of subsistence, in accordance with applicable provisions under subchapter I of chapter 57 of title 5, United States Code.

(F) EXECUTIVE SECRETARY.—The Director may appoint an executive secretary, who shall be an employee of the National Reconnaissance Office, to support the Board.

(4) MEETINGS.—The Board shall meet not less than quarterly, but may meet more frequently at the call of the Director.

(5) REPORTS.—Not later than March 31 of each year, the Board shall submit to the Director and to the congressional intelligence committees a report on the activities and significant findings of the Board during the preceding year.

- (6) NONAPPLICABILITY OF CERTAIN REQUIREMENTS.—The Federal Advisory Committee Act (5 U.S.C. App.) shall not apply to the Board.
- (7) TERMINATION.—The Board shall terminate on September 30, 2024.

ANNUAL NATIONAL SECURITY STRATEGY REPORT

SEC. 108. [50 U.S.C. § 3043]

(a)(1) The President shall transmit to Congress each year a comprehensive report on the national security strategy of the United States (hereinafter in this section referred to as a “national security strategy report”).

(2) The national security strategy report for any year shall be transmitted on the date on which the President submits to Congress the budget for the next fiscal year under section 1105 of title 31, United States Code.

(3) Not later than 150 days after the date on which a new President takes office, the President shall transmit to Congress a national security strategy report under this section. That report shall be in addition to the report for that year transmitted at the time specified in paragraph (2).

(b) Each national security strategy report shall set forth the national security strategy of the United States and shall include a comprehensive description and discussion of the following:

(1) The worldwide interests, goals, and objectives of the United States that are vital to the national security of the United States.

(2) The foreign policy, worldwide commitments, and national defense capabilities of the United States necessary to deter aggression and to implement the national security strategy of the United States.

(3) The proposed short-term and long-term uses of the political, economic, military, and other elements of the national power of the United States to protect or promote the interests and achieve the goals and objectives referred to in paragraph (1).

(4) The adequacy of the capabilities of the United States to carry out the national security strategy of the United States, including an evaluation of the balance among the capabilities of all elements of the national power of the United States to support the implementation of the national security strategy.

(5) Such other information as may be necessary to help inform Congress on matters relating to the national security strategy of the United States.

(c) Each national security strategy report shall be transmitted to Congress in classified form, but may include an unclassified summary.

NATIONAL INTELLIGENCE STRATEGY

SEC. 108A. [50 U.S.C. § 3043a]

(a) **IN GENERAL.**—Beginning in 2017, and once every 4 years thereafter, the Director of National Intelligence shall develop a comprehensive national intelligence strategy to meet national security objectives for the following 4-year period, or a longer period, if appropriate.

(b) **REQUIREMENTS.**—Each national intelligence strategy required by subsection (a) shall—

- (1) delineate a national intelligence strategy consistent with—
 - (A) the most recent national security strategy report submitted pursuant to section 108;
 - (B) the strategic plans of other relevant departments and agencies of the United States; and
 - (C) other relevant national-level plans;
- (2) address matters related to national and military intelligence, including counterintelligence;
- (3) identify the major national security missions that the intelligence community is currently pursuing and will pursue in the future to meet the anticipated security environment;
- (4) describe how the intelligence community will utilize personnel, technology, partnerships, and other capabilities to pursue the major national security missions identified in paragraph (3);
- (5) assess current, emerging, and future threats to the intelligence community, including threats from foreign intelligence and security services and insider threats;
- (6) outline the organizational roles and missions of the elements of the intelligence community as part of an integrated enterprise to meet customer demands for intelligence products, services, and support;
- (7) identify sources of strategic, institutional, programmatic, fiscal, and technological risk; and
- (8) analyze factors that may affect the intelligence community's performance in pursuing the major national security missions identified in paragraph (3) during the following 10-year period.

(c) **SUBMISSION TO CONGRESS.**—The Director of National Intelligence shall submit to the congressional intelligence committees a report on each national intelligence strategy required by subsection (a) not later than 45 days after the date of the completion of such strategy.

ANNUAL REPORTS ON WORLDWIDE THREATS

SEC. 108B. [50 U.S.C. § 3043b]

(a) **DEFINITION OF APPROPRIATE CONGRESSIONAL COMMITTEES.**—In this section, the term ‘appropriate congressional committees’ means—

- (1) the congressional intelligence committees; and
- (2) the Committees on Armed Services of the House of Representatives and the Senate.

(b) **ANNUAL REPORTS.**—Not later than the first Monday in February 2021, and each year thereafter, the Director of National Intelligence, in coordination with the heads of the elements of the intelligence community, shall submit to the appropriate congressional committees a report containing an assessment of the intelligence community with respect to worldwide threats to the national security of the United States.

(c) **FORM.**—Each report under subsection (b) shall be submitted in unclassified form, but may include a classified annex only for the protection of intelligence sources and methods relating to the matters contained in the report.

(d) **HEARINGS.**—

(1) **OPEN HEARINGS.**—Upon request by the appropriate congressional committees, the Director (and any other head of an element of the intelligence community determined appropriate by the committees in consultation with the Director) shall testify before such committees in an open setting regarding a report under subsection (b).

(2) **CLOSED HEARINGS.**—Any information that may not be disclosed during an open hearing under paragraph (1) in order to protect intelligence sources and methods may instead be discussed in a closed hearing that immediately follows such open hearing.

SOFTWARE LICENSING

SEC. 109. [50 U.S.C. § 3044]

(a) **REQUIREMENT FOR INVENTORIES OF SOFTWARE LICENSES.**—The chief information officer of each element of the intelligence community, in consultation with the Chief Information Officer of the Intelligence Community, shall biennially—

- (1) conduct an inventory of all existing software licenses of such element, including utilized and unutilized licenses;
- (2) assess the actions that could be carried out by such element to achieve the greatest possible economies of scale and associated cost savings in software procurement and usage, including—

(A) increasing the centralization of the management of software licenses;

(B) increasing the regular tracking and maintaining of comprehensive inventories of software licenses using automated discovery and inventory tools and metrics;

(C) analyzing software license data to inform investment decisions; and

(D) providing appropriate personnel with sufficient software licenses management training; and

(3) submit to the Chief Information Officer of the Intelligence Community each inventory required by paragraph (1) and each assessment required by paragraph (2).

(b) INVENTORIES BY THE CHIEF INFORMATION OFFICER OF THE INTELLIGENCE COMMUNITY.—The Chief Information Officer of the Intelligence Community, based on the inventories and assessments required by subsection (a), shall biennially—

(1) compile an inventory of all existing software licenses of the intelligence community, including utilized and unutilized licenses;

(2) assess the actions that could be carried out by the intelligence community to achieve the greatest possible economies of scale and associated cost savings in software procurement and usage, including—

(A) increasing the centralization of the management of software licenses;

(B) increasing the regular tracking and maintaining of comprehensive inventories of software licenses using automated discovery and inventory tools and metrics;

(C) analyzing software license data to inform investment decisions; and

(D) providing appropriate personnel with sufficient software licenses management training; and

(3) based on the assessment required under paragraph (2), make such recommendations with respect to software procurement and usage to the Director of National Intelligence as the Chief Information Officer considers appropriate.

(c) REPORTS TO CONGRESS.—The Chief Information Officer of the Intelligence Community shall submit to the congressional intelligence committees a copy of each inventory compiled under subsection (b)(1).

(d) IMPLEMENTATION OF RECOMMENDATIONS.—Not later than 180 days after the date on which the Director of National Intelligence receives recommendations from the Chief Information Officer of the Intelligence Community in accordance with subsection (b)(3), the Director of National Intelligence shall, to the extent practicable, issue guidelines for the intelligence community on software procurement and usage based on such recommendations.

NATIONAL MISSION OF NATIONAL GEOSPATIAL-INTELLIGENCE AGENCY

SEC. 110. [50 U.S.C. § 3045]

(a) **IN GENERAL.**—In addition to the Department of Defense missions set forth in section 442 of title 10, United States Code, the National Geospatial-Intelligence Agency shall support the geospatial intelligence requirements of the Department of State and other departments and agencies of the United States outside the Department of Defense.

(b) **REQUIREMENTS AND PRIORITIES.**—The Director of National Intelligence shall establish requirements and priorities governing the collection of national intelligence by the National Geospatial-Intelligence Agency under subsection (a).

(c) **CORRECTION OF DEFICIENCIES.**—The Director of National Intelligence shall develop and implement such programs and policies as the Director and the Secretary of Defense jointly determine necessary to review and correct deficiencies identified in the capabilities of the National Geospatial-Intelligence Agency to accomplish assigned national missions, including support to the all-source analysis and production process. The Director shall consult with the Secretary of Defense on the development and implementation of such programs and policies. The Secretary shall obtain the advice of the Chairman of the Joint Chiefs of Staff regarding the matters on which the Director and the Secretary are to consult under the preceding sentence.

RESTRICTIONS ON INTELLIGENCE SHARING WITH THE UNITED NATIONS

SEC. 112. [50 U.S.C. § 3047]

(a) **PROVISION OF INTELLIGENCE INFORMATION TO UNITED NATIONS.**—

(1) No United States intelligence information may be provided to the United Nations or any organization affiliated with the United Nations, or to any officials or employees thereof, unless the President certifies to the appropriate committees of Congress that the Director of National Intelligence, in consultation with the Secretary of State and the Secretary of Defense, has established and implemented procedures, and has worked with the United Nations to ensure implementation of procedures, for protecting from unauthorized disclosure United States intelligence sources and methods connected to such information.

(2) Paragraph (1) may be waived upon written certification by the President to the appropriate committees of Congress that providing such information to the United Nations or an organization affiliated with the United Nations, or to any officials or employees thereof, is in the national security interests of the United States.

(b) **DELEGATION OF DUTIES.**—The President may not delegate or assign the duties of the President under this section.

(c) RELATIONSHIP TO EXISTING LAW.—Nothing in this section shall be construed to—

- (1) impair or otherwise affect the authority of the Director of National Intelligence to protect intelligence sources and methods from unauthorized disclosure pursuant to section 102A(i) of this Act; or
- (2) supersede or otherwise affect the provisions of title V of this Act.

(d) DEFINITION.—As used in this section, the term “appropriate committees of Congress” means the Committee on Foreign Relations and the Select Committee on Intelligence of the Senate and the Committee on Foreign Relations and the Permanent Select Committee on Intelligence of the House of Representatives.

**DETAIL OF INTELLIGENCE COMMUNITY PERSONNEL-
INTELLIGENCE COMMUNITY ASSIGNMENT PROGRAM**

SEC. 113. [50 U.S.C. § 3048]

(a) DETAIL.—

(1) Notwithstanding any other provision of law, the head of a department with an element in the intelligence community or the head of an intelligence community agency or element may detail any employee within that department, agency, or element to serve in any position in the Intelligence Community Assignment Program on a reimbursable or a nonreimbursable basis.

(2) Nonreimbursable details may be for such periods as are agreed to between the heads of the parent and host agencies, up to a maximum of three years, except that such details may be extended for a period not to exceed one year when the heads of the parent and host agencies determine that such extension is in the public interest.

(b) BENEFITS, ALLOWANCES, TRAVEL, INCENTIVES.—

(1) An employee detailed under subsection (a) may be authorized any benefit, allowance, travel, or incentive otherwise provided to enhance staffing by the organization from which the employee is detailed.

(2) The head of an agency of an employee detailed under subsection (a) may pay a lodging allowance for the employee subject to the following conditions:

(A) The allowance shall be the lesser of the cost of the lodging or a maximum amount payable for the lodging as established jointly by the Director of National Intelligence and—

- (i) with respect to detailed employees of the Department of Defense, the Secretary of Defense; and
- (ii) with respect to detailed employees of other agencies and departments, the head of such agency or department.

(B) The detailed employee maintains a primary residence for the employee's immediate family in the local commuting area of the parent agency duty station from which the employee regularly commuted to such duty station before the detail.

(C) The lodging is within a reasonable proximity of the host agency duty station.

(D) The distance between the detailed employee's parent agency duty station and the host agency duty station is greater than 20 miles.

(E) The distance between the detailed employee's primary residence and the host agency duty station is 10 miles greater than the distance between such primary residence and the employee's parent duty station.

(F) The rate of pay applicable to the detailed employee does not exceed the rate of basic pay for grade GS-15 of the General Schedule.

NON-REIMBURSABLE DETAIL OF OTHER PERSONNEL

SEC. 113A. [50 U.S.C. § 3049]

An officer or employee of the United States or member of the Armed Forces may be detailed to the staff of an element of the intelligence community funded through the National Intelligence Program from another element of the intelligence community or from another element of the United States Government on a non-reimbursable basis, as jointly agreed to by the heads of the receiving and detailing elements, for a period not to exceed three years. This section does not limit any other source of authority for reimbursable or non-reimbursable details. A non-reimbursable detail made under this section shall not be considered an augmentation of the appropriations of the receiving element of the intelligence community.

SPECIAL PAY AUTHORITY FOR SCIENCE, TECHNOLOGY, ENGINEERING OR MATHEMATICS POSITIONS AND POSITIONS REQUIRING BANKING OR FINANCIAL SERVICES EXPERTISE

SEC. 113B. [50 U.S.C. § 3049a]

(a) **SPECIAL RATES OF PAY FOR POSITIONS REQUIRING EXPERTISE IN SCIENCE, TECHNOLOGY, ENGINEERING, OR MATHEMATICS OR IN BANKING OR FINANCIAL SERVICES.**—

(1) **IN GENERAL.**—Notwithstanding part III of title 5, United States Code, the head of each element of the intelligence community may, for one or more categories of positions in such element that require expertise

in science, technology, engineering, or mathematics or in banking or financial services (including expertise relating to critical financial infrastructure operations, capital markets, banking compliance programs, or international investments)—

(A) establish higher minimum rates of pay; and

(B) make corresponding increases in all rates of pay of the pay range for each grade or level, subject to subsection (b) or (c) as applicable.

(2) LIMITATION ON NUMBER OF RECIPIENTS.—For each element of the intelligence community, the number of individuals serving in a position in such element who receive a higher rate of pay established or increased under paragraph (1) may not, at any time during a given fiscal year, exceed 50 individuals or 5 percent of the total number of full-time equivalent positions authorized for such element for the preceding fiscal year, whichever is greater.

(3) TREATMENT.—The special rate supplements resulting from the establishment of higher rates under paragraph (1) shall be basic pay for the same or similar purposes as those specified in section 5305(j) of title 5, United States Code.

(b) SPECIAL RATES OF PAY FOR CYBER POSITIONS.—

(1) IN GENERAL.—Notwithstanding subsection (c), the Director of the National Security Agency may establish a special rate of pay—

(A) not to exceed the rate of basic pay payable for level II of the Executive Schedule under section 5313 of title 5, United States Code, if the Director certifies to the Under Secretary of Defense for Intelligence and Security, in consultation with the Under Secretary of Defense for Personnel and Readiness, that the rate of pay is for positions that perform functions that execute the cyber mission of the Agency; or

(B) not to exceed the rate of basic pay payable for the Vice President of the United States under section 104 of title 3, United States Code, if the Director certifies to the Secretary of Defense, by name, individuals that have advanced skills and competencies and that perform critical functions that execute the cyber mission of the Agency.

(2) PAY LIMITATION.—Employees receiving a special rate under paragraph (1) shall be subject to an aggregate pay limitation that parallels the limitation established in section 5307 of title 5, United States Code, except that—

(A) any allowance, differential, bonus, award, or other similar cash payment in addition to basic pay that is authorized under title 10, United States Code, (or any other applicable law in

addition to title 5 of such Code, excluding the Fair Labor Standards Act of 1938 (29 U.S.C. 201 et seq.)) shall also be counted as part of aggregate compensation; and

(B) aggregate compensation may not exceed the rate established for the Vice President of the United States under section 104 of title 3, United States Code.

(3) **LIMITATION ON NUMBER OF RECIPIENTS.**—The number of individuals who receive basic pay established under paragraph (1)(B) may not exceed 100 at any time.

(4) **LIMITATION.**—Notwithstanding any other provision of law, special rates of pay and the limitation established under paragraph (1)(B) may not be used as comparative references for the purpose of fixing the rates of basic pay or maximum pay limitations of qualified positions under section 1599f of title 10, United States Code, or section 2208 of the Homeland Security Act of 2002 (6 U.S.C. 658).

(c) **MAXIMUM SPECIAL RATE OF PAY.**—Except as provided in subsection (b), a minimum rate of pay established for a category of positions under subsection (a) may not exceed the maximum rate of basic pay (excluding any locality-based comparability payment under section 5304 of Title 5, United States Code, or similar provision of law) for the position in that category of positions without the authority of subsection (a) by more than 30 percent, and no rate may be established under this section in excess of the rate of basic pay payable for level IV of the Executive Schedule under section 5315 of title 5, United States Code.

(d) **NOTIFICATION OF REMOVAL FROM SPECIAL RATE OF PAY.**—If the head of an element of the intelligence community removes a category of positions from coverage under a rate of pay authorized by subsection (a) or (b) after that rate of pay takes effect—

(1) the head of such element shall provide notice of the loss of coverage of the special rate of pay to each individual in such category; and

(2) the loss of coverage will take effect on the first day of the first pay period after the date of the notice.

(e) **REVISION OF SPECIAL RATES OF PAY.**—Subject to the limitations in this section, rates of pay established under this section by the head of an element of the intelligence community may be revised from time to time by the head of such element and the revisions have the force and effect of statute.

(f) **REGULATIONS.**—The head of each element of the intelligence community shall promulgate regulations to carry out this section with respect to such element, which shall, to the extent practicable, be comparable to the regulations promulgated to carry out section 5305 of title 5, United States Code.

(g) **REPORTS.**—

(1) **REQUIREMENT FOR REPORTS.**—Not later than 90 days after the date of the enactment of the Damon Paul Nelson and Matthew Young Pollard

Intelligence Authorization Act for Fiscal Years 2018 and 2019, the head of each element of the intelligence community shall submit to the congressional intelligence committees a report on any rates of pay established for such element under this section.

(2) CONTENTS.—Each report required by paragraph (1) shall contain for each element of the intelligence community—

(A) a description of any rates of pay established under subsection (a) or (b); and

(B) the number of positions in such element that will be subject to such rates of pay.

ANNUAL REPORT ON HIRING AND RETENTION OF MINORITY EMPLOYEES

SEC. 114. [50 U.S.C. § 3050]

(a) IN GENERAL.—The Director of National Intelligence shall, on an annual basis, submit to Congress a report on the employment of covered persons within each element of the intelligence community for the preceding fiscal year and the preceding 5 fiscal years.

(b) CONTENT.—Each such report shall include data, disaggregated by category of covered person and by element of the intelligence community, on the following:

(1) Of all individuals employed in the element during the fiscal year involved, the aggregate percentage of such individuals who are covered persons.

(2) Of all individuals employed in the element during the fiscal year involved at the levels referred to in subparagraphs (A) and (B), the percentage of covered persons employed at such levels:

(A) Positions at levels 1 through 15 of the General Schedule.

(B) Positions at levels above GS–15.

(3) Of all individuals hired by the element involved during the fiscal year involved, the percentage of such individuals who are covered persons.

(c) FORM.—Each such report shall be submitted in unclassified form, but may contain a classified annex.

(d) CONSTRUCTION.—Nothing in this section shall be construed as providing for the substitution of any similar report required under another provision of law.

(e) “COVERED PERSONS” DEFINED.—In this section, the term “covered persons” means—

(1) racial and ethnic minorities;

(2) women; and

(3) individuals with disabilities.

**LIMITATION ON ESTABLISHMENT OR OPERATION OF DIPLOMATIC
INTELLIGENCE SUPPORT CENTERS**

SEC. 115. [50 U.S.C. § 3052]

(a) IN GENERAL.—

(1) A diplomatic intelligence support center may not be established, operated, or maintained without the prior approval of the Director of National Intelligence.

(2) The Director may only approve the establishment, operation, or maintenance of a diplomatic intelligence support center if the Director determines that the establishment, operation, or maintenance of such center is required to provide necessary intelligence support in furtherance of the national security interests of the United States.

(b) PROHIBITION OF USE OF APPROPRIATIONS.—Amounts appropriated pursuant to authorizations by law for intelligence and intelligence-related activities may not be obligated or expended for the establishment, operation, or maintenance of a diplomatic intelligence support center that is not approved by the Director of National Intelligence.

(c) DEFINITIONS.—In this section:

(1) The term “diplomatic intelligence support center” means an entity to which employees of the various elements of the intelligence community (as defined in section 3(4)) are detailed for the purpose of providing analytical intelligence support that—

(A) consists of intelligence analyses on military or political matters and expertise to conduct limited assessments and dynamic taskings for a chief of mission; and

(B) is not intelligence support traditionally provided to a chief of mission by the Director of National Intelligence.

(2) The term “chief of mission” has the meaning given that term by section 102(3) of the Foreign Service Act of 1980 (22 U.S.C. 3902(3)), and includes ambassadors at large and ministers of diplomatic missions of the United States, or persons appointed to lead United States offices abroad designated by the Secretary of State as diplomatic in nature.

(d) TERMINATION.—This section shall cease to be effective on October 1, 2000.

**TRAVEL ON ANY COMMON CARRIER FOR
CERTAIN INTELLIGENCE COLLECTION PERSONNEL**

SEC. 116. [50 U.S.C. § 3053]

(a) IN GENERAL.—Notwithstanding any other provision of law, the Director of National Intelligence may authorize travel on any common carrier when such travel, in the discretion of the Director—

- (1) is consistent with intelligence community mission requirements, or
- (2) is required for cover purposes, operational needs, or other exceptional circumstances necessary for the successful performance of an intelligence community mission.

(b) **AUTHORIZED DELEGATION OF DUTY.**—The Director of National Intelligence may only delegate the authority granted by this section to the Principal Deputy Director of National Intelligence, or with respect to employees of the Central Intelligence Agency, to the Director of the Central Intelligence Agency, who may delegate such authority to other appropriate officials of the Central Intelligence Agency.

POW/MIA ANALYTIC CAPABILITY

SEC. 117. [50 U.S.C. § 3054]

(a) **REQUIREMENT.**—

- (1) The Director of National Intelligence shall, in consultation with the Secretary of Defense, establish and maintain in the intelligence community an analytic capability with responsibility for intelligence in support of the activities of the United States relating to individuals who, after December 31, 1990, are unaccounted for United States personnel.
- (2) The analytic capability maintained under paragraph (1) shall be known as the “POW/MIA analytic capability of the intelligence community”.

(b) **UNACCOUNTED FOR UNITED STATES PERSONNEL.**—In this section, the term “unaccounted for United States personnel” means the following:

- (1) Any missing person (as that term is defined in section 1513(1) of title 10, United States Code).
- (2) Any United States national who was killed while engaged in activities on behalf of the United States and whose remains have not been repatriated to the United States.

ANNUAL REPORT ON FINANCIAL INTELLIGENCE ON TERRORIST ASSETS

SEC. 118. [50 U.S.C. § 3055]

(a) **ANNUAL REPORT.**—On an annual basis, the Secretary of the Treasury (acting through the head of the Office of Intelligence Support) shall submit a report to the appropriate congressional committees that fully informs the committees concerning operations against terrorist financial networks.

Each such report shall include with respect to the preceding one-year period—

- (1) the total number of asset seizures, designations, and other actions against individuals or entities found to have engaged in financial support of terrorism;

- (2) the total number of physical searches of offices, residences, or financial records of individuals or entities suspected of having engaged in financial support for terrorist activity; and
- (3) whether the financial intelligence information seized in these cases has been shared on a full and timely basis with the all departments, agencies, and other entities of the United States Government involved in intelligence activities participating in the Foreign Terrorist Asset Tracking Center.

(b) IMMEDIATE NOTIFICATION FOR EMERGENCY DESIGNATION.—In the case of a designation of an individual or entity, or the assets of an individual or entity, as having been found to have engaged in terrorist activities, the Secretary of the Treasury shall report such designation within 24 hours of such a designation to the appropriate congressional committees.

(c) SUBMITTAL DATE OF REPORTS TO CONGRESSIONAL INTELLIGENCE COMMITTEES.—In the case of the reports required to be submitted under subsection (a) to the congressional intelligence committees, the submittal dates for such reports shall be as provided in section 507.

(d) APPROPRIATE CONGRESSIONAL COMMITTEES DEFINED.—In this section, the term “appropriate congressional committees” means the following:

- (1) The Permanent Select Committee on Intelligence, the Committee on Appropriations, the Committee on Armed Services, and the Committee on Financial Services of the House of Representatives.
- (2) The Select Committee on Intelligence, the Committee on Appropriations, the Committee on Armed Services, and the Committee on Banking, Housing, and Urban Affairs of the Senate.

NATIONAL COUNTERTERRORISM CENTER

SEC. 119. [50 U.S.C. § 3056]

(a) ESTABLISHMENT OF CENTER.—There is within the Office of the Director of National Intelligence a National Counterterrorism Center.

(b) DIRECTOR OF NATIONAL COUNTERTERRORISM CENTER.—

- (1) There is a Director of the National Counterterrorism Center, who shall be the head of the National Counterterrorism Center, and who shall be appointed by the President, by and with the advice and consent of the Senate.
- (2) The Director of the National Counterterrorism Center may not simultaneously serve in any other capacity in the executive branch.

(c) REPORTING.—

- (1) The Director of the National Counterterrorism Center shall report to the Director of National Intelligence with respect to matters described in

paragraph (2) and the President with respect to matters described in paragraph (3).

(2) The matters described in this paragraph are as follows:

(A) The budget and programs of the National Counterterrorism Center.

(B) The activities of the Directorate of Intelligence of the National Counterterrorism Center under subsection (i).

(C) The conduct of intelligence operations implemented by other elements of the intelligence community; and

(3) The matters described in this paragraph are the planning and progress of joint counterterrorism operations (other than intelligence operations).

(d) **PRIMARY MISSIONS.**—The primary missions of the National Counterterrorism Center shall be as follows:

(1) To serve as the primary organization in the United States Government for analyzing and integrating all intelligence possessed or acquired by the United States Government pertaining to terrorism and counterterrorism, excepting intelligence pertaining exclusively to domestic terrorists and domestic counterterrorism.

(2) To conduct strategic operational planning for counterterrorism activities, integrating all instruments of national power, including diplomatic, financial, military, intelligence, homeland security, and law enforcement activities within and among agencies.

(3) To assign roles and responsibilities as part of its strategic operational planning duties to lead Departments or agencies, as appropriate, for counterterrorism activities that are consistent with applicable law and that support counterterrorism strategic operational plans, but shall not direct the execution of any resulting operations.

(4) To ensure that agencies, as appropriate, have access to and receive all-source intelligence support needed to execute their counterterrorism plans or perform independent, alternative analysis.

(5) To ensure that such agencies have access to and receive intelligence needed to accomplish their assigned activities.

(6) To serve as the central and shared knowledge bank on known and suspected terrorists and international terror groups, as well as their goals, strategies, capabilities, and networks of contacts and support.

(e) **DOMESTIC COUNTERTERRORISM INTELLIGENCE.**—

(1) The Center may, consistent with applicable law, the direction of the President, and the guidelines referred to in section 102A(b), receive intelligence pertaining exclusively to domestic counterterrorism from any Federal, State, or local government or other source necessary to fulfill its responsibilities and retain and disseminate such intelligence.

(2) Any agency authorized to conduct counterterrorism activities may request information from the Center to assist it in its responsibilities, consistent with applicable law and the guidelines referred to in section 102A(b).

(f) DUTIES AND RESPONSIBILITIES OF DIRECTOR.—

(1) The Director of the National Counterterrorism Center shall—

(A) serve as the principal adviser to the Director of National Intelligence on intelligence operations relating to counterterrorism;

(B) provide strategic operational plans for the civilian and military counterterrorism efforts of the United States Government and for the effective integration of counterterrorism intelligence and operations across agency boundaries, both inside and outside the United States;

(C) advise the Director of National Intelligence on the extent to which the counterterrorism program recommendations and budget proposals of the departments, agencies, and elements of the United States Government conform to the priorities established by the President;

(D) disseminate terrorism information, including current terrorism threat analysis, to the President, the Vice President, the Secretaries of State, Defense, and Homeland Security, the Attorney General, the Director of the Central Intelligence Agency, and other officials of the executive branch as appropriate, and to the appropriate committees of Congress;

(E) support the Department of Justice and the Department of Homeland Security, and other appropriate agencies, in fulfillment of their responsibilities to disseminate terrorism information, consistent with applicable law, guidelines referred to in section 102A(b), Executive orders and other Presidential guidance, to State and local government officials, and other entities, and coordinate dissemination of terrorism information to foreign governments as approved by the Director of National Intelligence;

(F) develop a strategy for combining terrorist travel intelligence operations and law enforcement planning and operations into a cohesive effort to intercept terrorists, find terrorist travel facilitators, and constrain terrorist mobility;

(G) have primary responsibility within the United States Government for conducting net assessments of terrorist threats;

(H) consistent with priorities approved by the President, assist the Director of National Intelligence in establishing requirements

for the intelligence community for the collection of terrorism information; and

(I) perform such other duties as the Director of National Intelligence may prescribe or are prescribed by law.

(2) Nothing in paragraph (1)(G) shall limit the authority of the departments and agencies of the United States to conduct net assessments.

(g) LIMITATION.—The Director of the National Counterterrorism Center may not direct the execution of counterterrorism operations.

(h) RESOLUTION OF DISPUTES.—The Director of National Intelligence shall resolve disagreements between the National Counterterrorism Center and the head of a department, agency, or element of the United States Government on designations, assignments, plans, or responsibilities under this section. The head of such a department, agency, or element may appeal the resolution of the disagreement by the Director of National Intelligence to the President.

(i) DIRECTORATE OF INTELLIGENCE.—The Director of the National Counterterrorism Center shall establish and maintain within the National Counterterrorism Center a Directorate of Intelligence which shall have primary responsibility within the United States Government for analysis of terrorism and terrorist organizations (except for purely domestic terrorism and domestic terrorist organizations) from all sources of intelligence, whether collected inside or outside the United States.

(j) DIRECTORATE OF STRATEGIC OPERATIONAL PLANNING.—

(1) The Director of the National Counterterrorism Center shall establish and maintain within the National Counterterrorism Center a Directorate of Strategic Operational Planning which shall provide strategic operational plans for counterterrorism operations conducted by the United States Government.

(2) Strategic operational planning shall include the mission, objectives to be achieved, tasks to be performed, interagency coordination of operational activities, and the assignment of roles and responsibilities.

(3) The Director of the National Counterterrorism Center shall monitor the implementation of strategic operational plans, and shall obtain information from each element of the intelligence community, and from each other department, agency, or element of the United States Government relevant for monitoring the progress of such entity in implementing such plans.

NATIONAL COUNTERPROLIFERATION AND BIOSECURITY CENTER

SEC. 119A. [50 U.S.C. § 3057]

(a) ESTABLISHMENT.—

(1) The President shall establish a National Counterproliferation and Biosecurity Center, taking into account all appropriate government tools to—

(A) prevent and halt the proliferation of weapons of mass destruction, their delivery systems, and related materials and technologies; and

(B) lead integration and mission management of all intelligence activities pertaining to biosecurity and foreign biological threats.

(2) The head of the National Counterproliferation and Biosecurity Center shall be the Director of the National Counterproliferation and Biosecurity Center, who shall be appointed by the Director of National Intelligence.

(3) The National Counterproliferation and Biosecurity Center shall be located within the Office of the Director of National Intelligence.

(4) The Director of the National Counterproliferation and Biosecurity Center shall serve as the principal coordinator for the intelligence community, and as the principal advisor to the Director of National Intelligence, with respect to biosecurity and foreign biological threats.

(b) MISSIONS AND OBJECTIVES.—:

(1) COUNTERPROLIFERATION. —In establishing the National Counterproliferation and Biosecurity Center, the President shall address the following missions and objectives to prevent and halt the proliferation of weapons of mass destruction, their delivery systems, and related materials and technologies:

(A) Establishing a primary organization within the United States Government for analyzing and integrating all intelligence possessed or acquired by the United States pertaining to proliferation.

(B) Ensuring that appropriate agencies have full access to and receive all-source intelligence support needed to execute their counterproliferation plans or activities, and perform independent, alternative analyses.

(C) Establishing a central repository on known and suspected proliferation activities, including the goals, strategies, capabilities, networks, and any individuals, groups, or entities engaged in proliferation.

(D) Disseminating proliferation information, including proliferation threats and analyses, to the President, to the

appropriate departments and agencies, and to the appropriate committees of Congress.

(E) Conducting net assessments and warnings about the proliferation of weapons of mass destruction, their delivery systems, and related materials and technologies.

(F) Coordinating counterproliferation plans and activities of the various departments and agencies of the United States Government to prevent and halt the proliferation of weapons of mass destruction, their delivery systems, and related materials and technologies.

(G) Conducting strategic operational counterproliferation planning for the United States Government to prevent and halt the proliferation of weapons of mass destruction, their delivery systems, and related materials and technologies.

(2) BIOSECURITY. —In establishing the National Counterproliferation and Biosecurity Center, the President shall address the following missions and objectives to ensure that the Center serves as the lead for the intelligence community for the integration, mission management, and coordination of intelligence activities pertaining to biosecurity and foreign biological threats, regardless of origin:

(A) Ensuring that the elements of the intelligence community provide timely and effective warnings to the President and the Director of National Intelligence regarding emerging foreign biological threats, including diseases with pandemic potential.

(B) Overseeing and coordinating the collection and analysis of intelligence on biosecurity and foreign biological threats in support of the intelligence needs of the Federal departments and agencies responsible for public health, including by conveying collection priorities to elements of the intelligence community.

(C) Coordinating intelligence support to the Federal departments and agencies responsible for public health, including by ensuring that intelligence pertaining to biosecurity and foreign biological threats is disseminated among appropriately cleared personnel of such departments and agencies.

(D) Coordinating with the Federal departments and agencies responsible for public health to encourage information sharing with the intelligence community.

(E) Identifying gaps in the capabilities of the intelligence community regarding biosecurity and countering foreign biological threats and providing to the Director of National Intelligence recommended solutions for such gaps, including by encouraging

NATIONAL SECURITY ACT OF 1947

research and development of new capabilities to counter foreign biological threats.

(c) NATIONAL SECURITY WAIVER.—The President may waive the requirements of this section, and any parts thereof, if the President determines that such requirements do not materially improve the ability of the United States Government to prevent and halt the proliferation of weapons of mass destruction, their delivery systems, and related materials and technologies. Such waiver shall be made in writing to Congress and shall include a description of how the missions and objectives in subsection (b) are being met.

(d) REPORT TO CONGRESS.—

(1) Not later than nine months after the implementation of this Act, the President shall submit to Congress, in classified form if necessary, the findings and recommendations of the President's Commission on Weapons of Mass Destruction established by Executive Order in February 2004, together with the views of the President regarding the establishment of a National Counterproliferation and Biosecurity Center.

(2) If the President decides not to exercise the waiver authority granted by subsection (c), the President shall submit to Congress from time to time updates and plans regarding the establishment of a National Counterproliferation and Biosecurity Center.

(e) SENSE OF CONGRESS.—It is the sense of Congress that a central feature of counterproliferation activities, consistent with the President's Proliferation Security Initiative, should include the physical interdiction, by air, sea, or land, of weapons of mass destruction, their delivery systems, and related materials and technologies, and enhanced law enforcement activities to identify and disrupt proliferation networks, activities, organizations, and persons.

NATIONAL INTELLIGENCE CENTERS

SEC. 119B. [50 U.S.C. § 3058]

(a) AUTHORITY TO ESTABLISH.—The Director of National Intelligence may establish one or more national intelligence centers to address intelligence priorities, including, but not limited to, regional issues.

(b) RESOURCES OF DIRECTORS OF CENTERS.—

(1) The Director of National Intelligence shall ensure that the head of each national intelligence center under subsection (a) has appropriate authority, direction, and control of such center, and of the personnel assigned to such center, to carry out the assigned mission of such center.

(2) The Director of National Intelligence shall ensure that each national intelligence center has appropriate personnel to accomplish effectively the mission of such center.

(c) **INFORMATION SHARING.**—The Director of National Intelligence shall, to the extent appropriate and practicable, ensure that each national intelligence center under subsection (a) and the other elements of the intelligence community share information in order to facilitate the mission of such center.

(d) **MISSION OF CENTERS.**—Pursuant to the direction of the Director of National Intelligence, each national intelligence center under subsection (a) may, in the area of intelligence responsibility assigned to such center—

- (1) have primary responsibility for providing all-source analysis of intelligence based upon intelligence gathered both domestically and abroad;
- (2) have primary responsibility for identifying and proposing to the Director of National Intelligence, intelligence collection and analysis and production requirements; and
- (3) perform such other duties as the Director of National Intelligence shall specify.

(e) **REVIEW AND MODIFICATION OF CENTERS.**—The Director of National Intelligence shall determine on a regular basis whether—

- (1) the area of intelligence responsibility assigned to each national intelligence center under subsection (a) continues to meet appropriate intelligence priorities; and
- (2) the staffing and management of such center remains appropriate for the accomplishment of the mission of such center.

(f) **TERMINATION.**—The Director of National Intelligence may terminate any national intelligence center under subsection (a).

(g) **SEPARATE BUDGET ACCOUNT.**—The Director of National Intelligence shall, as appropriate, include in the National Intelligence Program budget a separate line item for each national intelligence center under subsection (a).

FOREIGN MALIGN INFLUENCE CENTER

SEC. 119C. [50 U.S.C. § [3059]]

(a) **ESTABLISHMENT.**—There is within the Office of the Director of National Intelligence a Foreign Malign Influence Center (in this section referred to as the “Center”).

(b) **FUNCTIONS AND COMPOSITION.**—The Center shall—

- (1) be comprised of analysts from all elements of the intelligence community, including elements with diplomatic and law enforcement functions;
- (2) have access to all intelligence and other reporting possessed or acquired by the United States Government pertaining to foreign malign influence;

- (3) serve as the primary organization in the United States Government for analyzing and integrating all intelligence possessed or acquired by the United States Government pertaining to foreign malign influence; and
- (4) provide to employees and officers of the Federal Government in policy-making positions and Congress comprehensive assessments, and indications and warnings, of foreign malign influence.

(c) DIRECTOR.—

(1) APPOINTMENT.—There is a Director of the Center, who shall be the head of the Center, and who shall be appointed by the Director of National Intelligence.

(2) ROLE.—The Director of the Center shall—

- (A) report directly to the Director of National Intelligence;
- (B) carry out the functions under subsection (b); and
- (C) at the request of the President or the Director of National Intelligence, develop and provide recommendations for potential responses by the United States to foreign malign influence.

(d) ANNUAL REPORTS.—

(1) IN GENERAL.—In addition to the matters submitted pursuant to subsection (b)(4), at the direction of the Director of National Intelligence, but not less than once each year, the Director of the Center shall submit to the congressional intelligence committees, the Committee on Foreign Affairs of the House of Representatives, and the Committee on Foreign Relations of the Senate a report on foreign malign influence.

(2) MATTERS INCLUDED.—Each report under paragraph (1) shall include, with respect to the period covered by the report, a discussion of the following:

- (A) The most significant activities of the Center.
- (B) Any recommendations the Director determines necessary for legislative or other actions to improve the ability of the Center to carry out its functions, including recommendations regarding the protection of privacy and civil liberties.

(e) TERMINATION. —After December 31, 2028, the Director of National Intelligence may terminate the Center, but only if the Director of National Intelligence submits to the congressional intelligence committees, the Subcommittee on Defense of the Committee on Appropriations of the Senate, and the Subcommittee on Defense of the Committee on Appropriations of the House of Representatives a determination that the termination of the Center is appropriate, which includes—

(1) a detailed description that other offices or entities within the intelligence community—

- (A) have the capabilities to perform the functions of the Center;
- and

(B) will exercise the functions of the Center upon the termination of the Center; and

(2) a detailed description of—

(A) the actions the Director of National Intelligence will take to conduct an orderly wind-down of the activities of the Center; and

(B) the proposed timeline for such actions.

(f) DEFINITIONS.—In this section:

(1) COVERED FOREIGN COUNTRY.—The term “covered foreign country” means the following:

(A) The Russian Federation.

(B) The Islamic Republic of Iran.

(C) The Democratic People’s Republic of Korea.

(D) The People’s Republic of China.

(E) Any other foreign country that the Director of the Center determines appropriate for purposes of this section.

(2) FOREIGN MALIGN INFLUENCE.—The term “foreign malign influence” means any hostile effort undertaken by, at the direction of, or on behalf of or with the substantial support of, the government of a covered foreign country with the objective of influencing, through overt or covert means—

(A) the political, military, economic, or other policies or activities of the United States Government or State or local governments, including any election within the United States; or

(B) the public opinion within the United States.

CLIMATE SECURITY ADVISORY COUNCIL

SEC. 120. [50 U.S.C. § [3060]

(a) ESTABLISHMENT.—The Director of National Intelligence shall establish a Climate Security Advisory Council for the purpose of—

(1) assisting intelligence analysts of various elements of the intelligence community with respect to analysis of climate security and its impact on the areas of focus of such analysts;

(2) facilitating coordination between the elements of the intelligence community and elements of the Federal Government that are not elements of the intelligence community in collecting data on, and conducting analysis of, climate change and climate security; and

(3) ensuring that the intelligence community is adequately prioritizing climate change in carrying out its activities.

(b) COMPOSITION OF COUNCIL.—

(1) MEMBERS.—The Council shall be composed of the following individuals appointed by the Director of National Intelligence:

NATIONAL SECURITY ACT OF 1947

- (A) An appropriate official from the National Intelligence Council, who shall chair the Council.
- (B) The lead official with respect to climate and environmental security analysis from—
 - (i) the Central Intelligence Agency;
 - (ii) the Bureau of Intelligence and Research of the Department of State;
 - (iii) the National Geospatial-Intelligence Agency;
 - (iv) the Office of Intelligence and Counterintelligence of the Department of Energy;
 - (v) the Office of the Under Secretary of Defense for Intelligence and Security; and
 - (vi) the Defense Intelligence Agency.
- (C) Three appropriate officials from elements of the Federal Government that are not elements of the intelligence community that are responsible for—
 - (i) providing decision makers with a predictive understanding of the climate;
 - (ii) making observations of our Earth system that can be used by the public, policymakers, and to support strategic decisions; or
 - (iii) coordinating Federal research and investments in understanding the forces shaping the global environment, both human and natural, and their impacts on society.
- (D) Any other officials as the Director of National Intelligence or the chair of the Council may determine appropriate.

(2) RESPONSIBILITIES OF CHAIR.—The chair of the Council shall have responsibility for—

- (A) identifying agencies to supply individuals from elements of the Federal Government that are not elements of the intelligence community;
- (B) securing the permission of the relevant agency heads for the participation of such individuals on the Council; and
- (C) any other duties that the Director of National Intelligence may direct.

(c) DUTIES AND RESPONSIBILITIES OF COUNCIL.—The Council shall carry out the following duties and responsibilities:

- (1) To meet at least quarterly to—
 - (A) exchange appropriate data between elements of the intelligence community and elements of the Federal Government that are not elements of the intelligence community;

- (B) discuss processes for the routine exchange of such data and implementation of such processes; and
- (C) prepare summaries of the business conducted at each meeting.

(2) To assess and determine best practices with respect to the analysis of climate security, including identifying publicly available information and intelligence acquired through clandestine means that enables such analysis.

(3) To assess and identify best practices with respect to prior efforts of the intelligence community to analyze climate security.

(4) To assess and describe best practices for identifying and disseminating climate intelligence indications and warnings.

(5) To recommend methods of incorporating analysis of climate security and the best practices identified under paragraphs (2) through (4) into existing analytic training programs.

(6) To consult, as appropriate, with other elements of the intelligence community that conduct analysis of climate change or climate security and elements of the Federal Government that are not elements of the intelligence community that conduct analysis of climate change or climate security, for the purpose of sharing information about ongoing efforts and avoiding duplication of existing efforts.

(7) To work with elements of the intelligence community that conduct analysis of climate change or climate security and elements of the Federal Government that are not elements of the intelligence community that conduct analysis of climate change or climate security—

- (A) to exchange appropriate data between such elements, establish processes, procedures and practices for the routine exchange of such data, discuss the implementation of such processes; and

- (B) to enable and facilitate the sharing of findings and analysis between such elements.

(8) To assess whether the elements of the intelligence community that conduct analysis of climate change or climate security may inform the research direction of academic work and the sponsored work of the United States Government.

(9) At the discretion of the chair of the Council, to convene conferences for analysts and non-intelligence community personnel working on climate change or climate security on subjects that the chair shall direct.

(d) ANNUAL REPORT.—

(1) REQUIREMENT. —Not later than January 31, 2021, and not less frequently than annually thereafter, the chair of the Council shall submit, on behalf of the Council, to the congressional intelligence committees a

report describing the activities of the Council as described in subsection (c) during the year preceding the year during which the report is submitted.

(2) **MATTERS INCLUDED.** —Each report under paragraph (1) shall include a description of any obstacles or gaps relating to—

(A) the Council fulfilling its duties and responsibilities under subsection (c); or

(B) the responsiveness of the intelligence community to the climate security needs and priorities of the policy-making elements of the Federal Government.

(e) **SUNSET.**—The Council shall terminate on December 31, 2024..

(f) **DEFINITIONS.**—In this section:

(1) **CLIMATE SECURITY.**—The term “climate security” means the effects of climate change on the following:

(A) The national security of the United States, including national security infrastructure.

(B) Subnational, national, and regional political stability.

(C) The security of allies and partners of the United States.

(D) Ongoing or potential political violence, including unrest, rioting, guerrilla warfare, insurgency, terrorism, rebellion, revolution, civil war, and interstate war.

(2) **CLIMATE INTELLIGENCE INDICATIONS AND WARNINGS.**—The term “climate intelligence indications and warnings” means developments relating to climate security with the potential to—

(A) imminently and substantially alter the political stability or degree of human security in a country or region; or

(B) imminently and substantially threaten—

(i) the national security of the United States;

(ii) the military, political, or economic interests of allies and partners of the United States; or

(iii) citizens of the United States abroad.

**COUNTERINTELLIGENCE AND NATIONAL SECURITY
PROTECTIONS FOR INTELLIGENCE COMMUNITY GRANT
FUNDING.**

SEC. 121. [50 U.S.C. § 3061]

(a) **DISCLOSURE AS CONDITION FOR RECEIPT OF GRANT.** —The head of an element of the intelligence community may not award a grant to a person or entity unless the person or entity has certified to the head of the element that the person or entity has disclosed to the head of the element any material financial or material in-kind support that the person or entity knows, or should have known,

derives from the People's Republic of China, the Russian Federation, the Islamic Republic of Iran, the Democratic People's Republic of Korea, or the Republic of Cuba, during the 5-year period ending on the date of the person or entity's application for the grant.

(b) PROCESS FOR REVIEW OF GRANT APPLICANTS PRIOR TO AWARD.—

(1) IN GENERAL. —The head of an element of the intelligence community may not award a grant to a person or entity who submitted a certification under subsection (a) until such certification is received by the head of an element of the intelligence community and submitted to the Director of National Intelligence pursuant to the process set forth in paragraph (2).

(2) PROCESS.—

(A) IN GENERAL. —The Director of National Intelligence, in coordination with such heads of elements of the intelligence community as the Director considers appropriate, shall establish a process to review the awarding of a grant to an applicant who submitted a certification under subsection (a).

(B) ELEMENTS. —The process established under subparagraph

(A) shall include the following:

(i) The immediate transmission of a copy of each applicant's certification made under subsection (a) to the Director of National Intelligence.

(ii) The review of the certification and any accompanying disclosures submitted under subsection (a) as soon as practicable.

(iii) Authorization for the heads of the elements of the intelligence community to take such actions as may be necessary, including denial or revocation of a grant, to ensure a grant does not pose an unacceptable risk of—

(I) misappropriation of United States intellectual property, research and development, and innovation efforts; or

(II) other counterintelligence threats.

(c) ANNUAL REPORT REQUIRED. —Not later than 1 year after the date of the enactment of the Intelligence Authorization Act for Fiscal Year 2023 and not less frequently than once each year thereafter, the Director of National Intelligence shall submit to the congressional intelligence committees an annual report identifying the following for the 1-year period covered by the report:

(1) The number of applications for grants received by each element of the intelligence community.

(2) The number of such applications that were reviewed using the process established under subsection (b)(2), disaggregated by element of the intelligence community.

(3) The number of such applications that were denied and the number of grants that were revoked, pursuant to the process established under subsection (b)(2), disaggregated by element of the intelligence community.

OFFICE OF ENGAGEMENT

SEC. 122. [50 U.S.C. § 3062]

(a) **ESTABLISHMENT.**—There is within the Office of the Director of National Intelligence an Office of Engagement (in this section referred to as the “Office”).

(b) **HEAD; STAFF.**—

(1) **HEAD.**—The Director of National Intelligence shall appoint as head of the Office an individual with requisite experience in matters relating to the duties of the Office, as determined by the Director of National Intelligence. Such head of the Office shall report directly to the Director of National Intelligence.

(2) **STAFF.**—To assist the head of the Office in fulfilling the duties of the Office, the head shall employ full-time equivalent staff in such number, and with such requisite expertise in matters relating to such duties, as may be determined by the head.

(c) **DUTIES.**—The duties of the Office shall be as follows:

(1) To ensure coordination across the elements of the intelligence community efforts regarding outreach, relationship development, and associated knowledge and relationship management, with covered entities, consistent with the protection of intelligence sources and methods.

(2) To assist in sharing best practices regarding such efforts among the elements of the intelligence community.

(3) To establish and implement metrics to assess the effectiveness of such efforts.

(d) **COVERED ENTITY DEFINED.**—In this section, the term “covered entity” means an entity that is not an entity of the United States Government, including private sector companies, institutions of higher education, trade associations, think tanks, laboratories, international organizations, and foreign partners and allies.

TITLE II—THE DEPARTMENT OF DEFENSE

DEPARTMENT OF DEFENSE

SEC. 201. [50 U.S.C. § 3005]

Except to the extent inconsistent with the provisions of this Act or other provisions of law, the provisions of title 5, United States Code, shall be applicable to the Department of Defense.

DEPARTMENT OF THE ARMY

SEC. 205. [50 U.S.C. § 3004]

(a) All laws, orders, regulations, and other actions relating to the Department of War or to any officer or activity whose title is changed under this section shall, insofar as they are not inconsistent with the provisions of this Act, be deemed to relate to the Department of the Army within the Department of Defense or to such officer or activity designated by his or its new title.

(b) The term “Department of the Army” as used in this Act shall be construed to mean the Department of the Army at the seat of government and all field headquarters, forces, reserve components, installations, activities, and functions under the control or supervision of the Department of the Army.

DEPARTMENT OF THE NAVY

SEC. 206. [50 U.S.C. § 3004]

The term “Department of the Navy” as used in this Act shall be construed to mean the Department of the Navy at the seat of government; the headquarters, United States Marine Corps; the entire operating forces of the United States Navy, including naval aviation, and of the United States Marine Corps, including the reserve components of such forces; all field activities, headquarters, forces, bases, installations, activities and functions under the control or supervision of the Department of the Navy; and the United States Coast Guard when operating as a part of the Navy pursuant to law.

DEPARTMENT OF THE AIR FORCE

SEC. 207. [50 U.S.C. § 3004]

The term “Department of the Air Force” as used in this Act shall be construed to mean the Department of the Air Force at the seat of government and all field headquarters, forces, reserve components, installations, activities, and functions under the control or supervision of the Department of the Air Force.

TITLE III—MISCELLANEOUS PROVISIONS

NATIONAL SECURITY AGENCY VOLUNTARY SEPARATION

SEC. 301. [50 U.S.C. § 3071]

(a) **SHORT TITLE.**—This section may be cited as the “National Security Agency Voluntary Separation Act”.

(b) **DEFINITIONS.**—For purposes of this section—

(1) the term “Director” means the Director of the National Security Agency; and

(2) the term “employee” means an employee of the National Security Agency, serving under an appointment without time limitation, who has been currently employed by the National Security Agency for a continuous period of at least 12 months prior to the effective date of the program established under subsection (c), except that such term does not include—

(A) a reemployed annuitant under subchapter III of chapter 83 or chapter 84 of title 5, United States Code, or another retirement system for employees of the Government; or

(B) an employee having a disability on the basis of which such employee is or would be eligible for disability retirement under any of the retirement systems referred to in subparagraph (A).

(c) **ESTABLISHMENT OF PROGRAM.**—Notwithstanding any other provision of law, the Director, in his sole discretion, may establish a program under which employees may, after October 1, 2000, be eligible for early retirement, offered separation pay to separate from service voluntarily, or both.

(d) **EARLY RETIREMENT.**—An employee who—

(1) is at least 50 years of age and has completed 20 years of service; or

(2) has at least 25 years of service, may, pursuant to regulations promulgated under this section, apply and be retired from the National Security Agency and receive benefits in accordance with chapter 83 or 84 of title 5, United States Code, if the employee has not less than 10 years of service with the National Security Agency.

(e) **AMOUNT OF SEPARATION PAY AND TREATMENT FOR OTHER PURPOSES.**—

(1) **AMOUNT.**—Separation pay shall be paid in a lump sum and shall be equal to the lesser of—

(A) an amount equal to the amount the employee would be entitled to receive under section 5595(c) of title 5, United States Code, if the employee were entitled to payment under such section; or

(B) \$25,000.

(2) TREATMENT.—Separation pay shall not—

- (A) be a basis for payment, and shall not be included in the computation, of any other type of Government benefit; and
- (B) be taken into account for the purpose of determining the amount of any severance pay to which an individual may be entitled under section 5595 of title 5, United States Code, based on any other separation.

(f) REEMPLOYMENT RESTRICTIONS.—An employee who receives separation pay under such program may not be reemployed by the National Security Agency for the 12-month period beginning on the effective date of the employee's separation. An employee who receives separation pay under this section on the basis of a separation occurring on or after the date of the enactment of the Federal Workforce Restructuring Act of 1994 (Public Law 103-236; 108 Stat. 111) and accepts employment with the Government of the United States within 5 years after the date of the separation on which payment of the separation pay is based shall be required to repay the entire amount of the separation pay to the National Security Agency. If the employment is with an Executive agency (as defined by section 105 of title 5, United States Code), the Director of the Office of Personnel Management may, at the request of the head of the agency, waive the repayment if the individual involved possesses unique abilities and is the only qualified applicant available for the position. If the employment is with an entity in the legislative branch, the head of the entity or the appointing official may waive the repayment if the individual involved possesses unique abilities and is the only qualified applicant available for the position. If the employment is with the judicial branch, the Director of the Administrative Office of the United States Courts may waive the repayment if the individual involved possesses unique abilities and is the only qualified applicant available for the position.

(g) BAR ON CERTAIN EMPLOYMENT.—

(1) BAR.—An employee may not be separated from service under this section unless the employee agrees that the employee will not—

- (A) act as agent or attorney for, or otherwise represent, any other person (except the United States) in any formal or informal appearance before, or, with the intent to influence, make any oral or written communication on behalf of any other person (except the United States) to the National Security Agency; or
- (B) participate in any manner in the award, modification, or extension of any contract for property or services with the National Security Agency, during the 12-month period beginning on the effective date of the employee's separation from service.

(2) PENALTY.—An employee who violates an agreement under this subsection shall be liable to the United States in the amount of the separation pay paid to the employee pursuant to this section multiplied

by the proportion of the 12-month period during which the employee was in violation of the agreement.

(h) **LIMITATIONS.**—Under this program, early retirement and separation pay may be offered only—

- (1) with the prior approval of the Director;
- (2) for the period specified by the Director; and
- (3) to employees within such occupational groups or geographic locations, or subject to such other similar limitations or conditions, as the Director may require.

(i) **REGULATIONS.**—Before an employee may be eligible for early retirement, separation pay, or both, under this section, the Director shall prescribe such regulations as may be necessary to carry out this section.

(j) **NOTIFICATION OF EXERCISE OF AUTHORITY.**—The Director may not make an offer of early retirement, separation pay, or both, pursuant to this section until 15 days after submitting to the congressional intelligence committees a report describing the occupational groups or geographic locations, or other similar limitations or conditions, required by the Director under subsection (h), and including the proposed regulations issued pursuant to subsection (i).

(k) **REMITTANCE OF FUNDS.**—In addition to any other payment that is required to be made under subchapter III of chapter 83 or chapter 84 of title 5, United States Code, the National Security Agency shall remit to the Office of Personnel Management for deposit in the Treasury of the United States to the credit of the Civil Service Retirement and Disability Fund, an amount equal to 15 percent of the final basic pay of each employee to whom a voluntary separation payment has been or is to be paid under this section. The remittance required by this subsection shall be in lieu of any remittance required by section 4(a) of the Federal Workforce Restructuring Act of 1994 (5 U.S.C. 8331 note).

**AUTHORITY OF FEDERAL BUREAU OF INVESTIGATION
TO AWARD PERSONAL SERVICES CONTRACTS**

SEC. 302. [50 U.S.C. § 3072]

(a) **IN GENERAL.**—The Director of the Federal Bureau of Investigation may enter into personal services contracts if the personal services to be provided under such contracts directly support the intelligence or counterintelligence missions of the Federal Bureau of Investigation.

(b) **INAPPLICABILITY OF CERTAIN REQUIREMENTS.**—Contracts under subsection (a) shall not be subject to the annuity offset requirements of sections 8344 and 8468 of title 5, United States Code, the requirements of section 3109 of title 5, United States Code, or any law or regulation requiring competitive contracting.

(c) **CONTRACT TO BE APPROPRIATE MEANS OF SECURING SERVICES.**—The Chief Contracting Officer of the Federal Bureau of Investigation shall ensure that each

personal services contract entered into by the Director under this section is the appropriate means of securing the services to be provided under such contract.

ADVISORY COMMITTEES AND PERSONNEL

SEC. 303. [50 U.S.C. § 3073]

(a) The Director of the Office of Defense Mobilization, the Director of National Intelligence, and the National Security Council, acting through its Executive Secretary, are authorized to appoint such advisory committees and to employ, consistent with other provisions of this Act, such part-time advisory personnel as they may deem necessary in carrying out their respective functions and the functions of agencies under their control. Persons holding other offices or positions under the United States for which they receive compensation, while serving as members of such committees, shall receive no additional compensation for such service. Retired members of the uniformed services employed by the Director of National Intelligence who hold no other office or position under the United States for which they receive compensation, other members of such committees and other part-time advisory personnel so employed may serve without compensation or may receive compensation at a daily rate not to exceed the daily equivalent of the rate of pay in effect for grade GS-18 of the General Schedule established by section 5332 of title 5, United States Code, as determined by the appointing authority.

(b) Service of an individual as a member of any such advisory committee, or in any other part-time capacity for a department or agency hereunder, shall not be considered as service bringing such individual within the provisions of section 203, 205, or 207, of title 18, United States Code, unless the act of such individual, which by such section is made unlawful when performed by an individual referred to in such section, is with respect to any particular matter which directly involves a department or agency which such person is advising or in which such department or agency is directly interested.

REQUIREMENTS FOR CERTAIN EMPLOYMENT ACTIVITIES BY FORMER INTELLIGENCE OFFICERS AND EMPLOYEES .

SEC. 304 [50 U.S.C. § 3073a]

(a) TEMPORARY RESTRICTION.—

(1) COVERED POST-SERVICE POSITION. —

(A) PERMANENT RESTRICTION.—Except as provided by paragraph (2)(A)(i), an employee of an element of the intelligence community who occupies a covered intelligence position may not occupy a covered post-service position for a designated prohibited foreign

country following the date on which the employee ceases to occupy a covered intelligence position.

(B) TEMPORARY RESTRICTION. —Except as provided by paragraph (2)(A)(ii), an employee of an element of the intelligence community who occupies a covered intelligence position may not occupy a covered post-service position during the 30-month period following the date on which the employee ceases to occupy a covered intelligence position.

(2) WAIVER.—

(A) Authority to grant temporary waiver.—

(i) WAIVERS OF PERMANENT RESTRICTION. —On a case-by-case basis, the Director of National Intelligence may temporarily waive the restriction in paragraph (1)(A) with respect to an employee or former employee who is subject to that restriction only after—

(I) the employee or former employee submits to the Director a written application for such waiver in such form and manner as the Director determines appropriate; and

(II) the Director determines that not granting such waiver would result in a grave detrimental impact to current or future intelligence operations of the United States; and

(III) the Director provides the congressional intelligence committees with a detailed justification stating why not granting such waiver would result in a grave detrimental impact to current or future intelligence operations of the United States.

(ii) WAIVERS OF TEMPORARY RESTRICTION.—On a case-by-case basis, the Director may temporarily waive the restriction in paragraph (1)(B) with respect to an employee or former employee who is subject to that restriction only after—

(I) the employee or former employee submits to the Director a written application for such waiver in such form and manner as the Director determines appropriate; and

(II) the Director determines that such waiver is necessary to advance the national security interests of the United States.

(B) PERIOD OF WAIVER.—A waiver issued under subparagraph (A) shall apply for a period not exceeding 5 years. The Director may renew such a waiver.

(C) REVOCATION.—The Director may revoke a waiver issued under subparagraph (A) to an employee or former employee, effective on the date that is 60 days after the date on which the Director provides the employee or former employee written notice of such revocation.

(D) TOLLING.—The 30-month restriction in paragraph (1)(B) shall be tolled for an employee or former employee during the period beginning on the date on which a waiver is issued under subparagraph (A) and ending on the date on which the waiver expires or on the effective date of a revocation under subparagraph (C), as the case may be.

(E) NOTIFICATION.—Not later than 30 days after the date on which the Director issues a waiver under subparagraph (A) or a revocation of a waiver under subparagraph (C), the Director shall submit to the congressional intelligence committees written notification of the waiver or revocation, as the case may be. Such notification shall include the following:

(i) With respect to a waiver issued to an employee or former employee—

(I) the details of the application, including the covered intelligence position held or formerly held by the employee or former employee;

(II) the nature of the activities of the employee or former employee after ceasing to occupy a covered intelligence position;

(III) a description of the national security interests that will be advanced by reason of issuing such waiver; and

(IV) the specific reasons why the Director determines that issuing such waiver will advance such interests.

(ii) With respect to a revocation of a waiver issued to an employee or former employee—

(I) the details of the waiver, including any renewals of such waiver, and the dates of such waiver and renewals; and

(II) the specific reasons why the Director determined that such revocation is warranted.

(b) COVERED POST-SERVICE EMPLOYMENT REPORTING. —

(1) REQUIREMENT. —During the period described in paragraph (2), an employee who ceases to occupy a covered intelligence position shall—

(A) report covered post-service employment to the head of the element of the intelligence community that employed such employee in such covered intelligence position upon accepting such covered post-service employment; and

(B) annually (or more frequently if the head of such element considers it appropriate) report covered post-service employment to the head of such element.

(2) PERIOD DESCRIBED. —The period described in this paragraph is the period beginning on the date on which an employee ceases to occupy a covered intelligence position.

(3) REGULATIONS. —The head of each element of the intelligence community shall issue regulations requiring, as a condition of employment, each employee of such element occupying a covered intelligence position to sign a written agreement requiring the regular reporting of covered post-service employment to the head of such element pursuant to paragraph (1).

(c) PENALTIES. —

(1) CRIMINAL PENALTIES. —A former employee who knowingly and willfully violates subsection (a) or who knowingly and willfully fails to make a required report under subsection (b) shall be fined under title 18, United States Code, or imprisoned for not more than 5 years, or both. Each report under subsection (b) shall be subject to section 1001 of title 18, United States Code.

(2) SECURITY CLEARANCES. —The head of an element of the intelligence community shall revoke the security clearance of a former employee if the former employee knowingly and willfully fails to make a required report under subsection (b) or knowingly and willfully makes a false report under such subsection.

(d) PROVISION OF INFORMATION. —

(1) TRAINING. —The head of each element of the intelligence community shall regularly provide training on the restrictions under subsection (a) and reporting requirements under subsection (b) to employees of that element who occupy a covered intelligence position.

(2) WRITTEN NOTICE ABOUT REPORTING REQUIREMENTS. —The head of each element of the intelligence community shall provide written notice of the reporting requirements under subsection (b) to an employee when the employee occupies a covered intelligence position.

(3) WRITTEN NOTICE ABOUT RESTRICTIONS. —The head of each element of the intelligence community shall provide written notice of the restrictions under subsection (a) to any person who may be

subject to such restrictions on or after the date of enactment of the Intelligence Authorization Act for Fiscal Year 2023—

(A) when the head of the element determines that such person may become subject to such covered intelligence position restrictions; and

(B) when the person occupies a covered intelligence position.'

(e) ANNUAL REPORTS. —

(1) REQUIREMENT. —Not later than March 31 of each year, the Director of National Intelligence shall submit to the congressional intelligence committees a report on covered post-service employment occurring during the year covered by the report.

(2) ELEMENTS. —Each report under paragraph (1) shall include the following:

(A) The number of former employees who occupy a covered post-service position, broken down by—

(i) the name of the employer;

(ii) the foreign government, including by the specific foreign individual, agency, or entity, for whom the covered post-service employment is being performed; and

(iii) the nature of the services provided as part of the covered post-service employment.

(B) A certification by the Director that—

(i) each element of the intelligence community maintains adequate systems and processes for ensuring that former employees are submitting reports required under subsection (b);

(ii) to the knowledge of the heads of the elements of the intelligence community, all former employees who occupy a covered post-service position are in compliance with this section;

(iii) the services provided by former employees who occupy a covered post-service position do not—

(I) pose a current or future threat to the national security of the United States; or

(II) post a counterintelligence risk; and

(iv) the Director and the heads of such elements are not aware of any credible information or reporting that any former employee who occupies a covered postservice position has engaged in activities that violate Federal law, infringe upon the privacy rights of United States persons, or constitute abuses of human rights.

(3) FORM. —Each report under paragraph (1) shall be submitted in unclassified form, but may include a classified annex.

(f) NOTIFICATION. —In addition to the annual reports under subsection (e), if a head of an element of the intelligence community determines that the services provided by a former employee who occupies a covered post-service position pose a threat or risk described in clause (iii) of paragraph (2)(B) of such subsection, or include activities described in clause (iv) of such paragraph, the head shall notify the congressional intelligence committees of such determination by not later than 7 days after making such determination. The notification shall include the following:

- (1) The name of the former employee.
- (2) The name of the employer.
- (3) The foreign government, including the specific foreign individual, agency, or entity, for whom the covered post-service employment is being performed.
- (4) As applicable, a description of —
 - (A) the risk to national security, the counterintelligence risk, or both; and
 - (B) the activities that may violate Federal law, infringe upon the privacy rights of United States persons, or constitute abuses of human rights.

(g) DEFINITIONS. —in this section.

(1) COVERED INTELLIGENCE POSITION.—The term “covered intelligence position” means a position within an element of the intelligence community that, based on the level of access of a person occupying such position to information regarding sensitive intelligence sources or methods or other exceptionally sensitive matters, the head of such element determines should be subject to the requirements of this section.

(2) COVERED POST-SERVICE EMPLOYMENT.—The term “covered post-service employment” means direct or indirect employment by, representation of, or any provision of advice or services relating to national security, intelligence, the military, or internal security to, the government of a foreign country or any company, entity, or other person whose activities are directly or indirectly supervised, directed, controlled, financed, or subsidized, in whole or in major part, by any government of a foreign country.

(3) COVERED POST-SERVICE POSITION.—The term “covered post-service position” means a position of employment described in paragraph (2).

(4) DESIGNATED PROHIBITED FOREIGN COUNTRY. —The term ‘designated prohibited foreign country’ means the following:

- (A) The People's Republic of China.
- (B) The Russian Federation.

- (C) The Democratic People's Republic of Korea.
- (D) The Islamic Republic of Iran.
- (E) The Republic of Cuba.
- (F) The Syrian Arab Republic.'

(5) **EMPLOYEE.**—The term “employee,” with respect to an employee occupying a covered intelligence position, includes an officer or official of an element of the intelligence community, a contractor of such an element, a detailee to such an element, or a member of the Armed Forces assigned to such an element.

(6) **FORMER EMPLOYEE.**—The term “former employee” means an individual—

(A) who was an employee occupying a covered intelligence position; and

(B) who is subject to the requirements under subsection (a) or (b).

(7) **GOVERNMENT OF A FOREIGN COUNTRY.**—The term “government of a foreign country” has the meaning given the term in section 1(e) of the Foreign Agents Registration Act of 1938 (22 U.S.C. 611(e)).

AUTHORIZATION FOR APPROPRIATIONS

SEC. 307. [50 U.S.C. § 3074]

There are hereby authorized to be appropriated such sums as may be necessary and appropriate to carry out the provisions and purposes of this Act (other than the provisions and purposes of sections 102, 103, 104, 105 and titles V, VI, and VII).

DEFINITIONS

SEC. 308. [50 U.S.C. § 3075]

(a) As used in sections 2, 101, 102, 103, and 303 of this Act, the term “function” includes functions, powers, and duties.

(b) As used in this Act, the term, “Department of Defense” shall be deemed to include the military departments of the Army, the Navy, and the Air Force, and all agencies created under title II of this Act.

SEPARABILITY

SEC. 309. [50 U.S.C. § 3076]

If any provision of this Act or the application thereof to any person or circumstances is held invalid, the validity of the remainder of the Act and of the

application of such provision to other persons and circumstances shall not be affected thereby.

EFFECTIVE DATE

SEC. 310. [50 U.S.C. § 3077]

(a) The first sentence of section 202(a) and sections 1, 2, 307, 308, 309, and 310 shall take effect immediately upon the enactment of this Act.

(b) Except as provided in subsection (a), the provisions of this Act shall take effect on whichever of the following days is the earlier: The day after the day upon which the Secretary of Defense first appointed takes office, or the sixtieth day after the date of the enactment of this Act.

REPEALING AND SAVING PROVISIONS

SEC. 312. [50 U.S.C. § 3006]

All laws, orders, and regulations inconsistent with the provisions of this title are repealed insofar as they are inconsistent with the powers, duties, and responsibilities enacted hereby: *Provided*, That the powers, duties, and responsibilities of the Secretary of Defense under this title shall be administered in conformance with the policy and requirements for administration of budgetary and fiscal matters in the Government generally, including accounting and financial reporting, and that nothing in this title shall be construed as eliminating or modifying the powers, duties, and responsibilities of any other department, agency, or officer of the Government in connection with such matters, but no such department, agency, or officer shall exercise any such powers, duties, or responsibilities in a manner that will render ineffective the provisions of this title.

INSIDER THREAT POLICY COMPLIANCE AND REPORTING

SEC. 313. [50 U.S.C. § 3078]

The head of each element of the intelligence community shall—

- (1) implement the policy established in accordance with section 102A(f)(8); and
- (2) concurrent with the submission to Congress of budget justification materials in support of the budget of the President for a fiscal year that is submitted to Congress under section 1105(a) of title 31, United States Code, submit to Congress a certification as to whether the element is in compliance with such policy.

TITLE V—ACCOUNTABILITY FOR INTELLIGENCE ACTIVITIES

GENERAL CONGRESSIONAL OVERSIGHT PROVISIONS

SEC. 501. [50 U.S.C. § 3091]

(a)(1) The President shall ensure that the congressional intelligence committees are kept fully and currently informed of the intelligence activities of the United States, including any significant anticipated intelligence activity as required by this title.

(2) Nothing in this title shall be construed as requiring the approval of the congressional intelligence committees as a condition precedent to the initiation of any significant anticipated intelligence activity.

(b) The President shall ensure that any illegal intelligence activity is reported promptly to the congressional intelligence committees, as well as any corrective action that has been taken or is planned in connection with such illegal activity.

(c) The President and the congressional intelligence committees shall each establish such written procedures as may be necessary to carry out the provisions of this title.

(d) The House of Representatives and the Senate shall each establish, by rule or resolution of such House, procedures to protect from unauthorized disclosure all classified information, and all information relating to intelligence sources and methods, that is furnished to the congressional intelligence committees or to Members of Congress under this title. Such procedures shall be established in consultation with the Director of National Intelligence. In accordance with such procedures, each of the congressional intelligence committees shall promptly call to the attention of its respective House, or to any appropriate committee or committees of its respective House, any matter relating to intelligence activities requiring the attention of such House or such committee or committees.

(e) Nothing in this Act shall be construed as authority to withhold information from the congressional intelligence committees on the grounds that providing the information to the congressional intelligence committees would constitute the unauthorized disclosure of classified information or information relating to intelligence sources and methods.

(f) As used in this section, the term “intelligence activities” includes covert actions as defined in section 503(e), and includes financial intelligence activities.

CONGRESSIONAL OVERSIGHT OF CONTROLLED ACCESS PROGRAMS

SEC. 501A. [U.S.C. § 3091a.]

(a) PERIODIC BRIEFINGS.—

(1) REQUIREMENT.—Not less frequently than semiannually or upon request by one of the appropriate congressional committees or a member

of congressional leadership, the Director of National Intelligence shall provide to such committees and congressional leadership a briefing on each controlled access program in effect.

(2) CONTENTS.—Each briefing provided under paragraph (1) shall include, at a minimum, the following:

(A) A description of the activity of the controlled access programs during the period covered by the briefing.

(B) Documentation with respect to how the controlled access programs have achieved outcomes consistent with requirements documented by the Director and, as applicable, the Secretary of Defense.

(b) LIMITATION ON ESTABLISHMENT.—A head of an element of the intelligence community may not establish a controlled access program, or a compartment or subcompartment therein, until the head notifies the appropriate congressional committees and congressional leadership of such controlled access program, compartment, or subcompartment, as the case may be.

(c) ANNUAL REPORTS.—

(1) REQUIREMENT.—On an annual basis, the head of each element of the intelligence community shall submit to the appropriate congressional committees and congressional leadership a report on controlled access programs administered by the head.

(2) MATTERS INCLUDED.—Each report submitted under paragraph (1) shall include, with respect to the period covered by the report, the following:

(A) A list of all compartments and subcompartments of controlled access programs active as of the date of the report.

(B) A list of all compartments and subcompartments of controlled access programs terminated during the period covered by the report.

(C) With respect to the report submitted by the Director of National Intelligence, in addition to the matters specified in clauses (A) and (B)—

(i) a certification regarding whether the creation, validation, or substantial modification, including termination, for all existing and proposed controlled access programs, and the compartments and subcompartments within each, are substantiated and justified based on the information required by clause (ii); and

(ii) for each certification—

(I) the rationale for the revalidation, validation, or substantial modification, including termination, of each

controlled access program, compartment, and subcompartment;
(II) the identification of a control officer for each controlled access program; and
(III) a statement of protection requirements for each controlled access program.

(d) DEFINITIONS.—In this section:

(1) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term “appropriate congressional committees” means—

- (A) the congressional intelligence committees;
- (B) the Committee on Appropriations of the Senate; and
- (C) the Committee on Appropriations of the House of Representatives.

(2) CONGRESSIONAL LEADERSHIP.—The term “congressional leadership” means—

- (A) the majority leader of the Senate;
- (B) the minority leader of the Senate;
- (C) the Speaker of the House of Representatives; and
- (D) the minority leader of the House of Representatives.

(3) CONTROLLED ACCESS PROGRAM.—The term “controlled access program” means a program created or managed pursuant to Intelligence Community Directive 906, or successor directive.

REPORTING OF INTELLIGENCE ACTIVITIES OTHER THAN COVERT ACTIONS

SEC. 502. [50 U.S.C. § 3092]

(a) IN GENERAL.—To the extent consistent with due regard for the protection from unauthorized disclosure of classified information relating to sensitive intelligence sources and methods or other exceptionally sensitive matters, the Director of National Intelligence and the heads of all departments, agencies, and other entities of the United States Government involved in intelligence activities shall—

- (1) keep the congressional intelligence committees fully and currently informed of all intelligence activities, other than a covert action (as defined in section 503(e)), which are the responsibility of, are engaged in by, or are carried out for or on behalf of, any department, agency, or entity of the United States Government, including any significant anticipated intelligence activity and any significant intelligence failure; and
- (2) furnish the congressional intelligence committees any information or material concerning intelligence activities (including the legal basis under which the intelligence activity is being or was conducted), other

than covert actions, which is within their custody or control, and which is requested by either of the congressional intelligence committees in order to carry out its authorized responsibilities.

(b) **FORM AND CONTENTS OF CERTAIN REPORTS.**—Any report relating to a significant anticipated intelligence activity or a significant intelligence failure that is submitted to the congressional intelligence committees for purposes of subsection (a)(1) shall be in writing, and shall contain the following:

- (1) A concise statement of any facts pertinent to such report.
- (2) An explanation of the significance of the intelligence activity or intelligence failure covered by such report.

(c) **STANDARDS AND PROCEDURES FOR CERTAIN REPORTS.**—The Director of National Intelligence, in consultation with the heads of the departments, agencies, and entities referred to in subsection (a), shall establish standards and procedures applicable to reports covered by subsection (b).

PRESIDENTIAL APPROVAL AND REPORTING OF COVERT ACTIONS

SEC. 503. [50 U.S.C. § 3093]

(a) The President may not authorize the conduct of a covert action by departments, agencies, or entities of the United States Government unless the President determines such an action is necessary to support identifiable foreign policy objectives of the United States and is important to the national security of the United States, which determination shall be set forth in a finding that shall meet each of the following conditions:

- (1) Each finding shall be in writing, unless immediate action by the United States is required and time does not permit the preparation of a written finding, in which case a written record of the President's decision shall be contemporaneously made and shall be reduced to a written finding as soon as possible but in no event more than 48 hours after the decision is made.
- (2) Except as permitted by paragraph (1), a finding may not authorize or sanction a covert action, or any aspect of any such action, which already has occurred.
- (3) Each finding shall specify each department, agency, or entity of the United States Government authorized to fund or otherwise participate in any significant way in such action. Any employee, contractor, or contract agent of a department, agency, or entity of the United States Government other than the Central Intelligence Agency directed to participate in any way in a covert action shall be subject either to the policies and regulations of the Central Intelligence Agency, or to written policies or regulations adopted by such department, agency, or entity, to govern such participation.

(4) Each finding shall specify whether it is contemplated that any third party which is not an element of, or a contractor or contract agent of, the United States Government, or is not otherwise subject to United States Government policies and regulations, will be used to fund or otherwise participate in any significant way in the covert action concerned, or be used to undertake the covert action concerned on behalf of the United States.

(5) A finding may not authorize any action that would violate the Constitution or any statute of the United States.

(b) To the extent consistent with due regard for the protection from unauthorized disclosure of classified information relating to sensitive intelligence sources and methods or other exceptionally sensitive matters, the Director of National Intelligence and the heads of all departments, agencies, and entities of the United States Government involved in a covert action—

(1) shall keep the congressional intelligence committees fully and currently informed of all covert actions which are the responsibility of, are engaged in by, or are carried out for or on behalf of, any department, agency, or entity of the United States Government, including significant failures; and

(2) shall furnish to the congressional intelligence committees any information or material concerning covert actions (including the legal basis under which the covert action is being or was conducted) which is in the possession, custody, or control of any department, agency, or entity of the United States Government and which is requested by either of the congressional intelligence committees in order to carry out its authorized responsibilities.

(c)(1) The President shall ensure that any finding approved pursuant to subsection (a) shall be reported in writing to the congressional intelligence committees as soon as possible after such approval and before the initiation of the covert action authorized by the finding, except as otherwise provided in paragraph (2) and paragraph (3).

(2) If the President determines that it is essential to limit access to the finding to meet extraordinary circumstances affecting vital interests of the United States, the finding may be reported to the chairmen and ranking minority members of the congressional intelligence committees, the Speaker and minority leader of the House of Representatives, the majority and minority leaders of the Senate, and such other member or members of the congressional leadership as may be included by the President.

(3) Whenever a finding is not reported pursuant to paragraph (1) or (2) of this subsection, the President shall fully inform the congressional

intelligence committees in a timely fashion and shall provide a statement of the reasons for not giving prior notice.

(4) In a case under paragraph (1), (2), or (3), a copy of the finding, signed by the President, shall be provided to the chairman of each congressional intelligence committee.

(5)(A) When access to a finding, or a notification provided under subsection (d)(1), is limited to the Members of Congress specified in paragraph (2), a written statement of the reasons for limiting such access shall also be provided.

(B) Not later than 180 days after a statement of reasons is submitted in accordance with subparagraph (A) or this subparagraph, the President shall ensure that—

- (i) all members of the congressional intelligence committees are provided access to the finding or notification; or
- (ii) a statement of reasons that it is essential to continue to limit access to such finding or such notification to meet extraordinary circumstances affecting vital interests of the United States is submitted to the Members of Congress specified in paragraph (2).

(d)(1) The President shall ensure that the congressional intelligence committees, or, if applicable, the Members of Congress specified in subsection (c)(2), are notified in writing of any significant change in a previously approved covert action, or any significant undertaking pursuant to a previously approved finding, in the same manner as findings are reported pursuant to subsection (c).

(2) In determining whether an activity constitutes a significant undertaking for purposes of paragraph (1), the President shall consider whether the activity—

- (A) involves significant risk of loss of life;
- (B) requires an expansion of existing authorities, including authorities relating to research, development, or operations;
- (C) results in the expenditure of significant funds or other resources;
- (D) requires notification under section 504;
- (E) gives rise to a significant risk of disclosing intelligence sources or methods; or
- (F) presents a reasonably foreseeable risk of serious damage to the diplomatic relations of the United States if such activity were disclosed without authorization.

(e) As used in this title, the term “covert action” means an activity or activities of the United States Government to influence political, economic, or military conditions abroad, where it is intended that the role of the United States

Government will not be apparent or acknowledged publicly, but does not include—

- (1) activities the primary purpose of which is to acquire intelligence, traditional counterintelligence activities, traditional activities to improve or maintain the operational security of United States Government programs, or administrative activities;
- (2) traditional diplomatic or military activities or routine support to such activities;
- (3) traditional law enforcement activities conducted by United States Government law enforcement agencies or routine support to such activities; or
- (4) activities to provide routine support to the overt activities (other than activities described in paragraph (1), (2), or (3)) of other United States Government agencies abroad.

(f) No covert action may be conducted which is intended to influence United States political processes, public opinion, policies, or media.

(g)(1) In any case where access to a finding reported under subsection (c) or notification provided under subsection (d)(1) is not made available to all members of a congressional intelligence committee in accordance with subsection (c)(2), the President shall notify all members of such committee that such finding or such notification has been provided only to the members specified in subsection (c)(2).

(2) In any case where access to a finding reported under subsection (c) or notification provided under subsection (d)(1) is not made available to all members of a congressional intelligence committee in accordance with subsection (c)(2), the President shall provide to all members of such committee a general description regarding the finding or notification, as applicable, consistent with the reasons for not yet fully informing all members of such committee.

(3) The President shall maintain—

(A) a record of the members of Congress to whom a finding is reported under subsection (c) or notification is provided under subsection (d)(1) and the date on which each member of Congress receives such finding or notification; and

(B) each written statement provided under subsection (c)(5).

(h) For each type of activity undertaken as part of a covert action, the President shall establish in writing a plan to respond to the unauthorized public disclosure of that type of activity.

FUNDING OF INTELLIGENCE ACTIVITIES

SEC. 504. [50 U.S.C. § 3094]

(a) Appropriated funds available to an intelligence agency may be obligated or expended for an intelligence or intelligence-related activity only if—

(1) those funds were specifically authorized by Congress for use for such intelligence or intelligence-related activities; or

(2) in the case of funds from the Reserve for Contingencies of the Central Intelligence Agency and consistent with the provisions of section 503 of this Act concerning any significant anticipated intelligence activity, the Director of the Central Intelligence Agency has notified the appropriate congressional committees of the intent to make such funds available for such activity; or

(3) in the case of funds specifically authorized by the Congress for a different activity—

(A) the activity to be funded is a higher priority intelligence or intelligence-related activity;

(B) the use of such funds for such activity supports an emergent need, improves program effectiveness, or increases efficiency; and

(C) the Director of National Intelligence, the Secretary of Defense, or the Attorney General, as appropriate, has notified the appropriate congressional committees of the intent to make such funds available for such activity;

(4) nothing in this subsection prohibits obligation or expenditure of funds available to an intelligence agency in accordance with sections 1535 and 1536 of title 31, United States Code.

(b) Funds available to an intelligence agency may not be made available for any intelligence or intelligence-related activity for which funds were denied by the Congress.

(c) No funds appropriated for, or otherwise available to, any department, agency, or entity of the United States Government may be expended, or may be directed to be expended, for any covert action, as defined in section 503(e), unless and until a Presidential finding required by subsection (a) of section 503 has been signed or otherwise issued in accordance with that subsection.

(d)(1) Except as otherwise specifically provided by law, funds available to an intelligence agency that are not appropriated funds may be obligated or expended for an intelligence or intelligence-related activity only if those funds are used for activities reported to the appropriate congressional committees pursuant to procedures which identify—

(A) the types of activities for which nonappropriated funds may be expended; and

(B) the circumstances under which an activity must be reported as a significant anticipated intelligence activity before such funds can be expended.

(2) Procedures for purposes of paragraph (1) shall be jointly agreed upon by the congressional intelligence committees and, as appropriate, the Director of National Intelligence or the Secretary of Defense.

(e) As used in this section—

(1) the term “intelligence agency” means any department, agency, or other entity of the United States involved in intelligence or intelligence-related activities;

(2) the term “appropriate congressional committees” means the Permanent Select Committee on Intelligence and the Committee on Appropriations of the House of Representatives and the Select Committee on Intelligence and the Committee on Appropriations of the Senate; and

(3) the term “specifically authorized by the Congress” means that—

(A) the activity and the amount of funds proposed to be used for that activity were identified in a formal budget request to the Congress, but funds shall be deemed to be specifically authorized for that activity only to the extent that the Congress both authorized the funds to be appropriated for that activity and appropriated the funds for that activity; or

(B) although the funds were not formally requested, the Congress both specifically authorized the appropriation of the funds for the activity and appropriated the funds for the activity.

NOTICE TO CONGRESS OF CERTAIN TRANSFERS OF DEFENSE ARTICLES AND DEFENSE SERVICES

SEC. 505. [50 U.S.C. § 3095]

(a)(1) The transfer of a defense article or defense service, or the anticipated transfer in any fiscal year of any aggregation of defense articles or defense services, exceeding \$1,000,000 in value by an intelligence agency to a recipient outside that agency shall be considered a significant anticipated intelligence activity for the purpose of this title.

(2) Paragraph (1) does not apply if—

(A) the transfer is being made to a department, agency, or other entity of the United States (so long as there will not be a subsequent retransfer of the defense articles or defense services outside the United States Government in conjunction with an intelligence or intelligence-related activity); or

(B) the transfer—

(i) is being made pursuant to authorities contained in part II of the Foreign Assistance Act of 1961, the Arms Export Control Act, title 10 of the United States Code (including a law enacted pursuant to section 8677(a) of title 10), or the Federal Property and Administrative Services Act of 1949, and

(ii) is not being made in conjunction with an intelligence or intelligence-related activity.

(3) An intelligence agency may not transfer any defense articles or defense services outside the agency in conjunction with any intelligence or intelligence-related activity for which funds were denied by the Congress.

(b) As used in this section—

(1) the term “intelligence agency” means any department, agency, or other entity of the United States involved in intelligence or intelligence-related activities;

(2) the terms “defense articles” and “defense services” mean the items on the United States Munitions List pursuant to section 38 of the Arms Export Control Act (22 CFR part 121);

(3) the term “transfer” means—

(A) in the case of defense articles, the transfer of possession of those articles; and

(B) in the case of defense services, the provision of those services; and

(4) the term “value” means—

(A) in the case of defense articles, the greater of—

(i) the original acquisition cost to the United States Government, plus the cost of improvements or other modifications made by or on behalf of the Government; or

(ii) the replacement cost; and

(B) in the case of defense services, the full cost to the Government of providing the services.

**SPECIFICITY OF NATIONAL INTELLIGENCE PROGRAM BUDGET
AMOUNTS FOR COUNTERTERRORISM, COUNTERPROLIFERATION,
COUNTERNARCOTICS, AND COUNTERINTELLIGENCE**

SEC. 506. [50 U.S.C. § 3096]

(a) IN GENERAL.—The budget justification materials submitted to Congress in support of the budget of the President for a fiscal year that is submitted to Congress under section 1105(a) of title 31, United States Code, shall set forth

separately the aggregate amount requested for that fiscal year for the National Intelligence Program for each of the following:

- (1) Counterterrorism.
- (2) Counterproliferation.
- (3) Counternarcotics.
- (4) Counterintelligence.

(b) ELECTION OF CLASSIFIED OR UNCLASSIFIED FORM.—Amounts set forth under subsection (a) may be set forth in unclassified form or classified form, at the election of the Director of National Intelligence.

**BUDGET TREATMENT OF COSTS OF ACQUISITION OF
MAJOR SYSTEMS BY THE INTELLIGENCE COMMUNITY**

SEC. 506A. [50 U.S.C. § 3097]

(a) INDEPENDENT COST ESTIMATES.—

(1) The Director of National Intelligence shall, in consultation with the head of each element of the intelligence community concerned, prepare an independent cost estimate of the full life-cycle cost of development, procurement, and operation of each major system to be acquired by the intelligence community.

(2)(A) Each independent cost estimate for a major system shall, to the maximum extent practicable, specify the amount required to be appropriated and obligated to develop, procure, and operate the major system in each fiscal year of the proposed period of development, procurement, and operation of the major system.

(B) For major system acquisitions requiring a service or capability from another acquisition or program to deliver the end-to-end functionality for the intelligence community end users, independent cost estimates shall include, to the maximum extent practicable, all estimated costs across all pertinent elements of the intelligence community. For collection programs, such cost estimates shall include the cost of new analyst training, new hardware and software for data exploitation and analysis, and any unique or additional costs for data processing, storing, and power, space, and cooling across the life cycle of the program. If such costs for processing, exploitation, dissemination, and storage are scheduled to be executed in other elements of the intelligence community, the independent cost estimate shall identify and annotate such costs for such other elements accordingly.

(3)(A) In the case of a program of the intelligence community that qualifies as a major system, an independent cost estimate shall be

prepared before the submission to Congress of the budget of the President for the first fiscal year in which appropriated funds are anticipated to be obligated for the development or procurement of such major system.

(B) In the case of a program of the intelligence community for which an independent cost estimate was not previously required to be prepared under this section, including a program for which development or procurement commenced before the date of the enactment of the Intelligence Authorization Act for Fiscal Year 2004, if the aggregate future costs of development or procurement (or any combination of such activities) of the program will exceed \$500,000,000 (in current fiscal year dollars), the program shall qualify as a major system for purposes of this section, and an independent cost estimate for such major system shall be prepared before the submission to Congress of the budget of the President for the first fiscal year thereafter in which appropriated funds are anticipated to be obligated for such major system.

(4) The independent cost estimate for a major system shall be updated upon—

(A) the completion of any preliminary design review associated with the major system;

(B) any significant modification to the anticipated design of the major system; or

(C) any change in circumstances that renders the current independent cost estimate for the major system inaccurate.

(5) Any update of an independent cost estimate for a major system under paragraph (4) shall meet all requirements for independent cost estimates under this section, and shall be treated as the most current independent cost estimate for the major system until further updated under that paragraph.

(b) PREPARATION OF INDEPENDENT COST ESTIMATES.—

(1) The Director shall establish within the Office of the Director of National Intelligence for Community Management an office which shall be responsible for preparing independent cost estimates, and any updates thereof, under subsection (a), unless a designation is made under paragraph (2).

(2) In the case of the acquisition of a major system for an element of the intelligence community within the Department of Defense, the Director and the Secretary of Defense shall provide that the independent cost estimate, and any updates thereof, under subsection (a) of this section be

prepared by an entity jointly designated by the Director and the Secretary in accordance with section 2434(b)(1)(A) of title 10, United States Code.

(c) UTILIZATION IN BUDGETS OF PRESIDENT.—

(1) If the budget of the President requests appropriations for any fiscal year for the development or procurement of a major system by the intelligence community, the President shall, subject to paragraph (2), request in such budget an amount of appropriations for the development or procurement, as the case may be, of the major system that is equivalent to the amount of appropriations identified in the most current independent cost estimate for the major system for obligation for each fiscal year for which appropriations are requested for the major system in such budget.

(2) If the amount of appropriations requested in the budget of the President for the development or procurement of a major system is less than the amount of appropriations identified in the most current independent cost estimate for the major system for obligation for each fiscal year for which appropriations are requested for the major system in such budget, the President shall include in the budget justification materials submitted to Congress in support of such budget—

(A) an explanation for the difference between the amount of appropriations requested and the amount of appropriations identified in the most current independent cost estimate;

(B) a description of the importance of the major system to the national security;

(C) an assessment of the consequences for the funding of all programs of the National Intelligence Program in future fiscal years if the most current independent cost estimate for the major system is accurate and additional appropriations are required in future fiscal years to ensure the continued development or procurement of the major system, including the consequences of such funding shortfalls on the major system and all other programs of the National Intelligence Program; and

(D) such other information on the funding of the major system as the President considers appropriate.

(d) INCLUSION OF ESTIMATES IN BUDGET JUSTIFICATION MATERIALS.—The budget justification materials submitted to Congress in support of the budget of the President shall include the most current independent cost estimate under this section for each major system for which appropriations are requested in such budget for any fiscal year.

(e) DEFINITIONS.—In this section:

(1) The term “budget of the President” means the budget of the President for a fiscal year as submitted to Congress under section 1105(a) of title 31, United States Code.

(2)(A) The term “independent cost estimate” means a pragmatic and neutral analysis, assessment, and quantification of all costs and risks associated with the development, acquisition, procurement, operation, and sustainment of a major system across its proposed life cycle, which shall be based on programmatic and technical specifications provided by the office within the element of the intelligence community with primary responsibility for the development, procurement, or operation of the major system.

(B) In accordance with subsection (a)(2)(B), each independent cost estimate shall include all costs required across elements of the intelligence community to develop, acquire, procure, operate, and sustain the system to provide the end-to-end intelligence functionality of the system, including—

- (i) for collection programs, the cost of new analyst training, new hardware and software for data exploitation and analysis, and any unique or additional costs for data processing, storing, and power, space, and cooling across the life cycle of the program; and
- (ii) costs for processing, exploitation, dissemination, and storage scheduled to be executed in other elements of the intelligence community.

(3) The term “major system” means any significant program of an element of the intelligence community with projected total development and procurement costs exceeding \$500,000,000 (based on fiscal year 2010 constant dollars), which costs shall include all end-to-end program costs, including costs associated with the development and procurement of the program and any other costs associated with the development and procurement of systems required to support or utilize the program.

ANNUAL PERSONNEL LEVEL ASSESSMENTS FOR THE INTELLIGENCE COMMUNITY

SEC. 506B. [50 U.S.C. § 3098]

(a) **REQUIREMENT TO PROVIDE.**— The Director of National Intelligence shall, in consultation with the head of each element of the intelligence community, prepare an annual personnel level assessment for such element that assesses the personnel levels for such element for the fiscal year following the fiscal year in which the assessment is submitted.

(b) SCHEDULE.—Each assessment required by subsection (a) shall be submitted to the congressional intelligence committees each year at the time that the President submits to Congress the budget for a fiscal year pursuant to section 1105 of title 31, United States Code.

(c) CONTENTS.—Each assessment required by subsection (a) submitted during a fiscal year shall contain the following information for the element of the intelligence community concerned:

- (1) The budget submission for personnel costs for the upcoming fiscal year.
- (2) The dollar and percentage increase or decrease of such costs as compared to the personnel costs of the current fiscal year.
- (3) The dollar and percentage increase or decrease of such costs as compared to the personnel costs during the prior 5 fiscal years.
- (4) The number of full-time equivalent positions that is the basis for which personnel funds are requested for the upcoming fiscal year.
- (5) The numerical and percentage increase or decrease of the number referred to in paragraph (4) as compared to the number of full-time equivalent positions of the current fiscal year.
- (6) The numerical and percentage increase or decrease of the number referred to in paragraph (4) as compared to the number of full-time equivalent positions during the prior 5 fiscal years.
- (7) The best estimate of the number and costs of core contract personnel to be funded by the element for the upcoming fiscal year.
- (8) The numerical and percentage increase or decrease of such costs of core contract personnel as compared to the best estimate of the costs of core contract personnel of the current fiscal year.
- (9) The numerical and percentage increase or decrease of such number and such costs of core contract personnel as compared to the number and cost of core contract personnel during the prior 5 fiscal years.
- (10) A justification for the requested personnel and core contract personnel levels.
- (11) The best estimate of the number of intelligence collectors and analysts employed by each element of the intelligence community.
- (12) The best estimate of the number of intelligence collectors and analysts contracted by each element of the intelligence community and a description of the functions performed by such contractors.
- (13) A statement by the Director of National Intelligence that, based on current and projected funding, the element concerned will have sufficient—
 - (A) internal infrastructure to support the requested personnel and core contract personnel levels;

- (B) training resources to support the requested personnel levels; and
- (C) funding to support the administrative and operational activities of the requested personnel levels.

VULNERABILITY ASSESSMENTS OF MAJOR SYSTEMS

SEC. 506C. [50 U.S.C. § 3099]

(a) INITIAL VULNERABILITY ASSESSMENTS.—

(1)(A) Except as provided in subparagraph (B), the Director of National Intelligence shall conduct and submit to the congressional intelligence committees an initial vulnerability assessment for each major system and its significant items of supply—

- (i) except as provided in clause (ii), prior to the completion of Milestone B or an equivalent acquisition decision for the major system; or

- (ii) prior to the date that is 1 year after the date of the enactment of the Intelligence Authorization Act for Fiscal Year 2010, in the case of a major system for which Milestone B or an equivalent acquisition decision—

- (I) was completed prior to such date of enactment; or

- (II) is completed on a date during the 180-day period following such date of enactment.

(B) The Director may submit to the congressional intelligence committees an initial vulnerability assessment required by clause (ii) of subparagraph (A) not later than 180 days after the date such assessment is required to be submitted under such clause if the Director notifies the congressional intelligence committees of the extension of the submission date under this subparagraph and provides a justification for such extension.

(C) The initial vulnerability assessment of a major system and its significant items of supply shall include use of an analysis-based approach to—

- (i) identify vulnerabilities;
- (ii) define exploitation potential;
- (iii) examine the system's potential effectiveness;
- (iv) determine overall vulnerability; and
- (v) make recommendations for risk reduction.

(2) If an initial vulnerability assessment for a major system is not submitted to the congressional intelligence committees as required by paragraph (1), funds appropriated for the acquisition of the major system

may not be obligated for a major contract related to the major system. Such prohibition on the obligation of funds for the acquisition of the major system shall cease to apply on the date on which the congressional intelligence committees receive the initial vulnerability assessment.

(b) **SUBSEQUENT VULNERABILITY ASSESSMENTS.**—

(1) The Director of National Intelligence shall, periodically throughout the procurement of a major system or if the Director determines that a change in circumstances warrants the issuance of a subsequent vulnerability assessment, conduct a subsequent vulnerability assessment of each major system and its significant items of supply within the National Intelligence Program.

(2) Upon the request of a congressional intelligence committee, the Director of National Intelligence may, if appropriate, recertify the previous vulnerability assessment or may conduct a subsequent vulnerability assessment of a particular major system and its significant items of supply within the National Intelligence Program.

(3) Any subsequent vulnerability assessment of a major system and its significant items of supply shall include use of an analysis-based approach and, if applicable, a testing-based approach, to monitor the exploitation potential of such system and reexamine the factors described in clauses (i) through (v) of subsection (a)(1)(C).

(c) **MAJOR SYSTEM MANAGEMENT.**—The Director of National Intelligence shall give due consideration to the vulnerability assessments prepared for a given major system when developing and determining the National Intelligence Program budget.

(d) **CONGRESSIONAL OVERSIGHT.**—

(1) The Director of National Intelligence shall provide to the congressional intelligence committees a copy of each vulnerability assessment conducted under subsection (a) or (b) not later than 10 days after the date of the completion of such assessment.

(2) The Director of National Intelligence shall provide the congressional intelligence committees with a proposed schedule for subsequent periodic vulnerability assessments of a major system under subsection (b)(1) when providing such committees with the initial vulnerability assessment under subsection (a) of such system as required by paragraph (1).

(e) **DEFINITIONS.**—In this section:

(1) The term “item of supply” has the meaning given that term in section 4(10) of the Office of Federal Procurement Policy Act (41 U.S.C. 403(10)).

(2) The term “major contract” means each of the 6 largest prime, associate, or Government-furnished equipment contracts under a major

system that is in excess of \$40,000,000 and that is not a firm, fixed price contract.

(3) The term “major system” has the meaning given that term in section 506A(e).

(4) The term “Milestone B” means a decision to enter into major system development and demonstration pursuant to guidance prescribed by the Director of National Intelligence.

(5) The term “vulnerability assessment” means the process of identifying and quantifying vulnerabilities in a major system and its significant items of supply.

INTELLIGENCE COMMUNITY BUSINESS SYSTEM TRANSFORMATION

SEC. 506D. [50 U.S.C. § 3100]

(a) LIMITATION ON OBLIGATION OF FUNDS.—

(1) Subject to paragraph (3), no funds appropriated to any element of the intelligence community may be obligated for an intelligence community business system transformation that will have a total cost in excess of \$3,000,000 unless—

- (A) the Director of the Office of Business Transformation of the Office of the Director of National Intelligence makes a certification described in paragraph (2) with respect to such intelligence community business system transformation; and
- (B) such certification is approved by the board established under subsection (f).

(2) The certification described in this paragraph for an intelligence community business system transformation is a certification made by the Director of the Office of Business Transformation of the Office of the Director of National Intelligence that the intelligence community business system transformation—

- (A) complies with the enterprise architecture under subsection (b) and such other policies and standards that the Director of National Intelligence considers appropriate; or
- (B) is necessary—

- (i) to achieve a critical national security capability or address a critical requirement; or
- (ii) to prevent a significant adverse effect on a project that is needed to achieve an essential capability, taking into consideration any alternative solutions for preventing such adverse effect.

(3) With respect to a fiscal year after fiscal year 2010, the amount referred to in paragraph (1) in the matter preceding subparagraph

(A) shall be equal to the sum of—

(A) the amount in effect under such paragraph (1) for the preceding fiscal year (determined after application of this paragraph), plus

(B) such amount multiplied by the annual percentage increase in the consumer price index (all items; U.S. city average) as of September of the previous fiscal year.

(b) ENTERPRISE ARCHITECTURE FOR INTELLIGENCE COMMUNITY BUSINESS SYSTEMS.—

(1) The Director of National Intelligence shall, acting through the board established under subsection (f), develop and implement an enterprise architecture to cover all intelligence community business systems, and the functions and activities supported by such business systems. The enterprise architecture shall be sufficiently defined to effectively guide, constrain, and permit implementation of interoperable intelligence community business system solutions, consistent with applicable policies and procedures established by the Director of the Office of Management and Budget.

(2) The enterprise architecture under paragraph (1) shall include the following:

(A) An information infrastructure that will enable the intelligence community to—

(i) comply with all Federal accounting, financial management, and reporting requirements;

(ii) routinely produce timely, accurate, and reliable financial information for management purposes;

(iii) integrate budget, accounting, and program information and systems; and

(iv) provide for the measurement of performance, including the ability to produce timely, relevant, and reliable cost information.

(B) Policies, procedures, data standards, and system interface requirements that apply uniformly throughout the intelligence community.

(c) RESPONSIBILITIES FOR INTELLIGENCE COMMUNITY BUSINESS SYSTEM TRANSFORMATION.—The Director of National Intelligence shall be responsible for the entire life cycle of an intelligence community business system transformation, including review, approval, and oversight of the planning, design, acquisition, deployment, operation, and maintenance of the business system transformation.

(d) INTELLIGENCE COMMUNITY BUSINESS SYSTEM INVESTMENT REVIEW.—

(1) The Director of the Office of Business Transformation of the Office of the Director of National Intelligence shall establish and implement, not later than 60 days after the enactment of the Intelligence Authorization Act for Fiscal Year 2010, an investment review process for the intelligence community business systems for which the Director of the Office of Business Transformation is responsible.

(2) The investment review process under paragraph (1) shall—

(A) meet the requirements of section 11312 of title 40, United States Code; and

(B) specifically set forth the responsibilities of the Director of the Office of Business Transformation under such review process.

(3) The investment review process under paragraph (1) shall include the following elements:

(A) Review and approval by an investment review board (consisting of appropriate representatives of the intelligence community) of each intelligence community business system as an investment before the obligation of funds for such system.

(B) Periodic review, but not less often than annually, of every intelligence community business system investment.

(C) Thresholds for levels of review to ensure appropriate review of intelligence community business system investments depending on the scope, complexity, and cost of the system involved.

(D) Procedures for making certifications in accordance with the requirements of subsection (a)(2).

[e) Repealed.]

(f) INTELLIGENCE COMMUNITY BUSINESS SYSTEM TRANSFORMATION GOVERNANCE BOARD.—

(1) The Director of National Intelligence shall establish a board within the intelligence community business system transformation governance structure (in this subsection referred to as the “Board”).

(2) The Board shall—

(A) recommend to the Director policies and procedures necessary to effectively integrate all business activities and any transformation, reform, reorganization, or process improvement initiatives undertaken within the intelligence community;

(B) review and approve any major update of—

(i) the enterprise architecture developed under subsection (b); and

(ii) any plans for an intelligence community business systems modernization;

(C) manage cross-domain integration consistent with such enterprise architecture;

(D) coordinate initiatives for intelligence community business system transformation to maximize benefits and minimize costs for the intelligence community, and periodically report to the Director on the status of efforts to carry out an intelligence community business system transformation;

(E) ensure that funds are obligated for intelligence community business system transformation in a manner consistent with subsection (a); and

(F) carry out such other duties as the Director shall specify.

(g) **RELATION TO ANNUAL REGISTRATION REQUIREMENTS.**—Nothing in this section shall be construed to alter the requirements of section 8083 of the Department of Defense Appropriations Act, 2005 (Public Law 108-287; 118 Stat. 989), with regard to information technology systems (as defined in subsection (d) of such section).

(h) **RELATIONSHIP TO DEFENSE BUSINESS ENTERPRISE ARCHITECTURE.**—Nothing in this section shall be construed to exempt funds authorized to be appropriated to the Department of Defense from the requirements of section 2222 of title 10, United States Code, to the extent that such requirements are otherwise applicable.

(i) **RELATION TO CLINGER-COHEN ACT.**—

(1) Executive agency responsibilities in chapter 113 of title 40, United States Code, for any intelligence community business system transformation shall be exercised jointly by—

(A) the Director of National Intelligence and the Chief Information Officer of the Intelligence Community; and

(B) the head of the executive agency that contains the element of the intelligence community involved and the chief information officer of that executive agency.

(2) The Director of National Intelligence and the head of the executive agency referred to in paragraph (1)(B) shall enter into a Memorandum of Understanding to carry out the requirements of this section in a manner that best meets the needs of the intelligence community and the executive agency.

(j) **REPORTS.**—Not later than March 31 of each of the years 2011 through 2014, the Director of National Intelligence shall submit to the congressional intelligence committees a report on the compliance of the intelligence community with the requirements of this section. Each such report shall—

- (1) describe actions taken and proposed for meeting the requirements of subsection (a), including—
 - (A) specific milestones and actual performance against specified performance measures, and any revision of such milestones and performance measures; and
 - (B) specific actions on the intelligence community business system transformations submitted for certification under such subsection;
- (2) identify the number of intelligence community business system transformations that received a certification described in subsection (a)(2); and
- (3) describe specific improvements in business operations and cost savings resulting from successful intelligence community business systems transformation efforts.

(k) DEFINITIONS.—In this section:

- (1) The term “enterprise architecture” has the meaning given that term in section 3601(4) of title 44, United States Code.
- (2) The terms “information system” and “information technology” have the meanings given those terms in section 11101 of title 40, United States Code.
- (3) The term “intelligence community business system” means an information system, including a national security system, that is operated by, for, or on behalf of an element of the intelligence community, including a financial system, mixed system, financial data feeder system, and the business infrastructure capabilities shared by the systems of the business enterprise architecture, including people, process, and technology, that build upon the core infrastructure used to support business activities, such as acquisition, financial management, logistics, strategic planning and budgeting, installations and environment, and human resource management.
- (4) The term “intelligence community business system transformation” means—
 - (A) the acquisition or development of a new intelligence community business system; or
 - (B) any significant modification or enhancement of an existing intelligence community business system (other than necessary to maintain current services).
- (5) The term “national security system” has the meaning given that term in section 3542 of title 44, United States Code.
- (6) The term “Office of Business Transformation of the Office of the Director of National Intelligence” includes any successor office that assumes the functions of the Office of Business Transformation of the

Office of the Director of National Intelligence as carried out by the Office of Business Transformation on the date of the enactment of the Intelligence Authorization Act for Fiscal Year 2010.

REPORTS ON THE ACQUISITION OF MAJOR SYSTEMS

SEC. 506E. [50 U.S.C. § 3101]

(a) DEFINITIONS.—In this section:

(1) The term “cost estimate”—

(A) means an assessment and quantification of all costs and risks associated with the acquisition of a major system based upon reasonably available information at the time the Director establishes the 2010 adjusted total acquisition cost for such system pursuant to subsection (h) or restructures such system pursuant to section 506F(c); and

(B) does not mean an “independent cost estimate”.

(2) The term “critical cost growth threshold” means a percentage increase in the total acquisition cost for a major system of at least 25 percent over the total acquisition cost for the major system as shown in the current Baseline Estimate for the major system.

(3)(A) The term “current Baseline Estimate” means the projected total acquisition cost of a major system that is—

(i) approved by the Director, or a designee of the Director, at Milestone B or an equivalent acquisition decision for the development, procurement, and construction of such system;

(ii) approved by the Director at the time such system is restructured pursuant to section 506F(c); or

(iii) the 2010 adjusted total acquisition cost determined pursuant to subsection (h).

(B) A current Baseline Estimate may be in the form of an independent cost estimate.

(4) Except as otherwise specifically provided, the term “Director” means the Director of National Intelligence.

(5) The term “independent cost estimate” has the meaning given that term in section 506A(e).

(6) The term “major contract” means each of the 6 largest prime, associate, or Government-furnished equipment contracts under a major system that is in excess of \$40,000,000 and that is not a firm, fixed price contract.

(7) The term “major system” has the meaning given that term in section 506A(e).

(8) The term “Milestone B” means a decision to enter into major system development and demonstration pursuant to guidance prescribed by the Director.

(9) The term “program manager” means—

(A) the head of the element of the intelligence community that is responsible for the budget, cost, schedule, and performance of a major system; or

(B) in the case of a major system within the Office of the Director of National Intelligence, the deputy who is responsible for the budget, cost, schedule, and performance of the major system.

(10) The term “significant cost growth threshold” means the percentage increase in the total acquisition cost for a major system of at least 15 percent over the total acquisition cost for such system as shown in the current Baseline Estimate for such system.

(11) The term “total acquisition cost” means the amount equal to the total cost for development and procurement of, and system-specific construction for, a major system.

(b) MAJOR SYSTEM COST REPORTS.—

(1) The program manager for a major system shall, on a quarterly basis, submit to the Director a major system cost report as described in paragraph (2).

(2) A major system cost report shall include the following information (as of the last day of the quarter for which the report is made):

(A) The total acquisition cost for the major system.

(B) Any cost variance or schedule variance in a major contract for the major system since the contract was entered into.

(C) Any changes from a major system schedule milestones or performances that are known, expected, or anticipated by the program manager.

(D) Any significant changes in the total acquisition cost for development and procurement of any software component of the major system, schedule milestones for such software component of the major system, or expected performance of such software component of the major system that are known, expected, or anticipated by the program manager.

(3) Each major system cost report required by paragraph (1) shall be submitted not more than 30 days after the end of the reporting quarter.

(c) REPORTS FOR BREACH OF SIGNIFICANT OR CRITICAL COST GROWTH THRESHOLDS.—If the program manager of a major system for which a report has previously been submitted under subsection (b) determines at any time during a quarter that there is reasonable cause to believe that the total acquisition

cost for the major system has increased by a percentage equal to or greater than the significant cost growth threshold or critical cost growth threshold and if a report indicating an increase of such percentage or more has not previously been submitted to the Director, then the program manager shall immediately submit to the Director a major system cost report containing the information, determined as of the date of the report, required under subsection (b).

(d) NOTIFICATION TO CONGRESS OF COST GROWTH.—

(1) Whenever a major system cost report is submitted to the Director, the Director shall determine whether the current acquisition cost for the major system has increased by a percentage equal to or greater than the significant cost growth threshold or the critical cost growth threshold.

(2) If the Director determines that the current total acquisition cost has increased by a percentage equal to or greater than the significant cost growth threshold or critical cost growth threshold, the Director shall submit to Congress a Major System Congressional Report pursuant to subsection (e).

(e) REQUIREMENT FOR MAJOR SYSTEM CONGRESSIONAL REPORT.—

(1) Whenever the Director determines under subsection (d) that the total acquisition cost of a major system has increased by a percentage equal to or greater than the significant cost growth threshold for the major system, a Major System Congressional Report shall be submitted to Congress not later than 45 days after the date on which the Director receives the major system cost report for such major system.

(2) If the total acquisition cost of a major system (as determined by the Director under subsection (d)) increases by a percentage equal to or greater than the critical cost growth threshold for the program or subprogram, the Director shall take actions consistent with the requirements of section 506F.

(f) MAJOR SYSTEM CONGRESSIONAL REPORT ELEMENTS.—

(1) Except as provided in paragraph (2), each Major System Congressional Report shall include the following:

(A) The name of the major system.

(B) The date of the preparation of the report.

(C) The program phase of the major system as of the date of the preparation of the report.

(D) The estimate of the total acquisition cost for the major system expressed in constant base-year dollars and in current dollars.

(E) The current Baseline Estimate for the major system in constant base-year dollars and in current dollars.

(F) A statement of the reasons for any increase in total acquisition cost for the major system.

- (G) The completion status of the major system—
- (i) expressed as the percentage that the number of years for which funds have been appropriated for the major system is of the number of years for which it is planned that funds will be appropriated for the major system; and
 - (ii) expressed as the percentage that the amount of funds that have been appropriated for the major system is of the total amount of funds which it is planned will be appropriated for the major system.
- (H) The fiscal year in which the major system was first authorized and in which funds for such system were first appropriated by Congress.
- (I) The current change and the total change, in dollars and expressed as a percentage, in the total acquisition cost for the major system, stated both in constant base-year dollars and in current dollars.
- (J) The quantity of end items to be acquired under the major system and the current change and total change, if any, in that quantity.
- (K) The identities of the officers responsible for management and cost control of the major system.
- (L) The action taken and proposed to be taken to control future cost growth of the major system.
- (M) Any changes made in the performance or schedule milestones of the major system and the extent to which such changes have contributed to the increase in total acquisition cost for the major system.
- (N) The following contract performance assessment information with respect to each major contract under the major system:
- (i) The name of the contractor.
 - (ii) The phase that the contract is in at the time of the preparation of the report.
 - (iii) The percentage of work under the contract that has been completed.
 - (iv) Any current change and the total change, in dollars and expressed as a percentage, in the contract cost.
 - (v) The percentage by which the contract is currently ahead of or behind schedule.
 - (vi) A narrative providing a summary explanation of the most significant occurrences, including cost and schedule variances under major contracts of the major system, contributing to the changes identified and a

discussion of the effect these occurrences will have on the future costs and schedule of the major system.

(O) In any case in which one or more problems with a software component of the major system significantly contributed to the increase in costs of the major system, the action taken and proposed to be taken to solve such problems.

(2) A Major System Congressional Report prepared for a major system for which the increase in the total acquisition cost is due to termination or cancellation of the entire major system shall include only—

(A) the information described in subparagraphs (A) through (F) of paragraph (1); and

(B) the total percentage change in total acquisition cost for such system.

(g) PROHIBITION ON OBLIGATION OF FUNDS.—If a determination of an increase by a percentage equal to or greater than the significant cost growth threshold is made by the Director under subsection (d) and a Major System Congressional Report containing the information described in subsection (f) is not submitted to Congress under subsection (e)(1), or if a determination of an increase by a percentage equal to or greater than the critical cost growth threshold is made by the Director under subsection (d) and the Major System Congressional Report containing the information described in subsection (f) and section 506F(b)(3) and the certification required by section 506F(b)(2) are not submitted to Congress under subsection (e)(2), funds appropriated for construction, research, development, test, evaluation, and procurement may not be obligated for a major contract under the major system. The prohibition on the obligation of funds for a major system shall cease to apply at the end of the 45-day period that begins on the date—

(1) on which Congress receives the Major System Congressional Report under subsection (e)(1) with respect to that major system, in the case of a determination of an increase by a percentage equal to or greater than the significant cost growth threshold (as determined in subsection (d)); or

(2) on which Congress receives both the Major System Congressional Report under subsection (e)(2) and the certification of the Director under section 506F(b)(2) with respect to that major system, in the case of an increase by a percentage equal to or greater than the critical cost growth threshold (as determined under subsection (d)).

(h) TREATMENT OF COST INCREASES PRIOR TO ENACTMENT OF INTELLIGENCE AUTHORIZATION ACT FOR FISCAL YEAR 2010.—

(1) Not later than 180 days after the date of the enactment of the Intelligence Authorization Act for Fiscal Year 2010, the Director—

(A) shall, for each major system, determine if the total acquisition cost of such major system increased by a percentage

equal to or greater than the significant cost growth threshold or the critical cost growth threshold prior to such date;

(B) shall establish for each major system for which the total acquisition cost has increased by a percentage equal to or greater than the significant cost growth threshold or the critical cost growth threshold prior to such date a revised current Baseline Estimate based upon an updated cost estimate;

(C) may, for a major system not described in subparagraph (B), establish a revised current Baseline Estimate based upon an updated cost estimate; and

(D) shall submit to Congress a report describing—

- (i) each determination made under subparagraph (A);
- (ii) each revised current Baseline Estimate established for a major system under subparagraph (B); and
- (iii) each revised current Baseline Estimate established for a major system under subparagraph (C), including the percentage increase of the total acquisition cost of such major system that occurred prior to the date of the enactment of the Intelligence Authorization Act for Fiscal Year 2010.

(2) The revised current Baseline Estimate established for a major system under subparagraph (B) or (C) of paragraph (1) shall be the 2010 adjusted total acquisition cost for the major system and may include the estimated cost of conducting any vulnerability assessments for such major system required under section 506C.

(i) **REQUIREMENTS TO USE BASE YEAR DOLLARS.**—Any determination of a percentage increase under this section shall be stated in terms of constant base year dollars.

(j) **FORM OF REPORT.**—Any report required to be submitted under this section may be submitted in a classified form.

CRITICAL COST GROWTH IN MAJOR SYSTEMS

SEC. 506F. [50 U.S.C. § 3102]

(a) **REASSESSMENT OF MAJOR SYSTEM.**—If the Director of National Intelligence determines under section 506E(d) that the total acquisition cost of a major system has increased by a percentage equal to or greater than the critical cost growth threshold for the major system, the Director shall—

- (1) determine the root cause or causes of the critical cost growth, in accordance with applicable statutory requirements, policies, procedures, and guidance; and
- (2) carry out an assessment of—

- (A) the projected cost of completing the major system if current requirements are not modified;
- (B) the projected cost of completing the major system based on reasonable modification of such requirements;
- (C) the rough order of magnitude of the costs of any reasonable alternative system or capability; and
- (D) the need to reduce funding for other systems due to the growth in cost of the major system.

(b) PRESUMPTION OF TERMINATION.—

(1) After conducting the reassessment required by subsection (a) with respect to a major system, the Director shall terminate the major system unless the Director submits to Congress a Major System Congressional Report containing a certification in accordance with paragraph (2) and the information described in paragraph (3). The Director shall submit such Major System Congressional Report and certification not later than 90 days after the date the Director receives the relevant major system cost report under subsection (b) or (c) of section 506E.

(2) A certification described by this paragraph with respect to a major system is a written certification that—

- (A) the continuation of the major system is essential to the national security;
- (B) there are no alternatives to the major system that will provide acceptable capability to meet the intelligence requirement at less cost;
- (C) the new estimates of the total acquisition cost have been determined by the Director to be reasonable;
- (D) the major system is a higher priority than other systems whose funding must be reduced to accommodate the growth in cost of the major system; and
- (E) the management structure for the major system is adequate to manage and control the total acquisition cost.

(3) A Major System Congressional Report accompanying a written certification under paragraph (2) shall include, in addition to the requirements of section 506E(e), the root cause analysis and assessment carried out pursuant to subsection (a), the basis for each determination made in accordance with subparagraphs (A) through (E) of paragraph (2), and a description of all funding changes made as a result of the growth in the cost of the major system, including reductions made in funding for other systems to accommodate such cost growth, together with supporting documentation.

(c) ACTIONS IF MAJOR SYSTEM NOT TERMINATED.—If the Director elects not to terminate a major system pursuant to subsection (b), the Director shall—

- (1) restructure the major system in a manner that addresses the root cause or causes of the critical cost growth, as identified pursuant to subsection (a), and ensures that the system has an appropriate management structure as set forth in the certification submitted pursuant to subsection (b)(2)(E);
- (2) rescind the most recent Milestone approval for the major system;
- (3) require a new Milestone approval for the major system before taking any action to enter a new contract, exercise an option under an existing contract, or otherwise extend the scope of an existing contract under the system, except to the extent determined necessary by the Milestone Decision Authority, on a nondelegable basis, to ensure that the system may be restructured as intended by the Director without unnecessarily wasting resources;
- (4) establish a revised current Baseline Estimate for the major system based upon an updated cost estimate; and
- (5) conduct regular reviews of the major system.

(d) **ACTIONS IF MAJOR SYSTEM TERMINATED.**—If a major system is terminated pursuant to subsection (b), the Director shall submit to Congress a written report setting forth—

- (1) an explanation of the reasons for terminating the major system;
- (2) the alternatives considered to address any problems in the major system; and
- (3) the course the Director plans to pursue to meet any intelligence requirements otherwise intended to be met by the major system.

(e) **FORM OF REPORT.**—Any report or certification required to be submitted under this section may be submitted in a classified form.

(f) **WAIVER.**—

(1) The Director may waive the requirements of subsections (d)(2), (e), and (g) of section 506E and subsections (a)(2), (b), (c), and (d) of this section with respect to a major system if the Director determines that at least 90 percent of the amount of the current Baseline Estimate for the major system has been expended.

(2)(A) If the Director grants a waiver under paragraph (1) with respect to a major system, the Director shall submit to the congressional intelligence committees written notice of the waiver that includes—

- (i) the information described in section 506E(f); and
- (ii) if the current total acquisition cost of the major system has increased by a percentage equal to or greater than the critical cost growth threshold—

(I) a determination of the root cause or causes of the critical cost growth, as described in subsection (a)(1); and

(II) a certification that includes the elements described in subparagraphs (A), (B), and (E) of subsection (b)(2).

(B) The Director shall submit the written notice required by subparagraph (A) not later than 90 days after the date that the Director receives a major system cost report under subsection (b) or (c) of section 506E that indicates that the total acquisition cost for the major system has increased by a percentage equal to or greater than the significant cost growth threshold or critical cost growth threshold.

(g) DEFINITIONS.—In this section, the terms “cost estimate”, “critical cost growth threshold”, “current Baseline Estimate”, “major system”, and “total acquisition cost” have the meaning given those terms in section 506E(a).

FUTURE BUDGET PROJECTIONS

SEC. 506G. [50 U.S.C. § 3103]

(a) FUTURE YEAR INTELLIGENCE PLANS.—

(1) The Director of National Intelligence, with the concurrence of the Director of the Office of Management and Budget, shall provide to the congressional intelligence committees a Future Year Intelligence Plan, as described in paragraph (2), for—

(A) each expenditure center in the National Intelligence Program; and

(B) each major system in the National Intelligence Program.

(2)(A) A Future Year Intelligence Plan submitted under this subsection shall include the year-by-year proposed funding for each center or system referred to in subparagraph (A) or (B) of paragraph (1), for the budget year for which the Plan is submitted and not less than the 4 subsequent fiscal years.

(B) A Future Year Intelligence Plan submitted under subparagraph (B) of paragraph (1) for a major system shall include—

(i) the estimated total life-cycle cost of such major system; and

(ii) major milestones that have significant resource implications for such major system.

(b) LONG-TERM BUDGET PROJECTIONS.—

(1) The Director of National Intelligence, with the concurrence of the Director of the Office of Management and Budget, shall provide to the congressional intelligence committees a Long-term Budget Projection for each element of the intelligence community funded under the National

Intelligence Program acquiring a major system that includes the budget for such element for the 5-year period that begins on the day after the end of the last fiscal year for which year-by-year proposed funding is included in a Future Year Intelligence Plan for such major system in accordance with subsection (a)(2)(A).

(2) A Long-term Budget Projection submitted under paragraph (1) shall include—

(A) projections for the appropriate element of the intelligence community for—

(i) pay and benefits of officers and employees of such element;

(ii) other operating and support costs and minor acquisitions of such element;

(iii) research and technology required by such element;

(iv) current and planned major system acquisitions for such element;

(v) any future major system acquisitions for such element; and

(vi) any additional funding projections that the Director of National Intelligence considers appropriate;

(B) a budget projection based on effective cost and schedule execution of current or planned major system acquisitions and application of Office of Management and Budget inflation estimates to future major system acquisitions;

(C) any additional assumptions and projections that the Director of National Intelligence considers appropriate; and

(D) a description of whether, and to what extent, the total projection for each year exceeds the level that would result from applying the most recent Office of Management and Budget inflation estimate to the budget of that element of the intelligence community.

(c) **SUBMISSION TO CONGRESS.**—The Director of National Intelligence, with the concurrence of the Director of the Office of Management and Budget, shall submit to the congressional intelligence committees each Future Year Intelligence Plan or Long-term Budget Projection required under subsection (a) or (b) for a fiscal year at the time that the President submits to Congress the budget for such fiscal year pursuant to section 1105 of title 31, United States Code.

(d) **MAJOR SYSTEM AFFORDABILITY REPORT.**—

(1) The Director of National Intelligence, with the concurrence of the Director of the Office of Management and Budget, shall prepare a report on the acquisition of a major system funded under the National

Intelligence Program before the time that the President submits to Congress the budget for the first fiscal year in which appropriated funds are anticipated to be obligated for the development or procurement of such major system.

(2) The report on such major system shall include an assessment of whether, and to what extent, such acquisition, if developed, procured, and operated, is projected to cause an increase in the most recent Future Year Intelligence Plan and Long-term Budget Projection submitted under this section for an element of the intelligence community.

(3) The Director of National Intelligence shall update the report whenever an independent cost estimate must be updated pursuant to section 506A(a)(4).

(4) The Director of National Intelligence shall submit each report required by this subsection at the time that the President submits to Congress the budget for a fiscal year pursuant to section 1105 of title 31, United States Code.

(e) DEFINITIONS.—In this section:

(1) BUDGET YEAR.—The term “budget year” means the next fiscal year for which the President is required to submit to Congress a budget pursuant to section 1105 of title 31, United States Code.

(2) INDEPENDENT COST ESTIMATE; MAJOR SYSTEM.—The terms “independent cost estimate” and “major system” have the meaning given those terms in section 506A(e).

REPORTS ON SECURITY CLEARANCES

SEC. 506H. [50 U.S.C. § 3104]

(a) REPORT ON SECURITY CLEARANCE DETERMINATIONS.—

(1) Not later than February 1 of each year, the President shall submit to Congress a report on the security clearance process. Such report shall include, for each security clearance level—

(A) the number of employees of the United States Government who—

(i) held a security clearance at such level as of October 1 of the preceding year; and

(ii) were approved for a security clearance at such level during the preceding fiscal year; and

(B) the number of contractors to the United States Government who—

(i) held a security clearance at such level as of October 1 of the preceding year; and

(ii) were approved for a security clearance at such level during the preceding fiscal year.

(2) For purposes of paragraph (1), the President may consider—

(A) security clearances at the level of confidential and secret as one security clearance level; and

(B) security clearances at the level of top secret or higher as one security clearance level.

(b) INTELLIGENCE COMMUNITY REPORTS.—

(1)(A) Not later than March 1 of each year, the Director of National Intelligence shall submit a report to the congressional intelligence committees, the Committee on Homeland Security and Governmental Affairs of the Senate, the Committee on Homeland Security of the House of Representatives, and the Committee on Oversight and Reform of the House of Representatives regarding the security clearances processed by each element of the intelligence community during the preceding fiscal year.

(B) The Director shall submit to the Committee on Armed Services of the Senate and the Committee on Armed Services of the House of Representatives such portions of the report submitted under subparagraph (A) as the Director determines address elements of the intelligence community that are within the Department of Defense.

(C) Each report submitted under this paragraph shall separately identify security clearances processed for Federal employees and contractor employees sponsored by each such element.

(2) Each report submitted under paragraph (1)(A) shall include, for each element of the intelligence community for the fiscal year covered by the report, the following:

(A) The total number of initial security clearance background investigations sponsored for new applicants.

(B) The total number of security clearance periodic reinvestigations sponsored for existing employees.

(C) The total number of initial security clearance background investigations for new applicants that were adjudicated with notice of a determination provided to the prospective applicant, including—

(i) the total number of such adjudications that were adjudicated favorably and granted access to classified information; and

(ii) the total number of such adjudications that were adjudicated unfavorably and resulted in a denial or revocation of a security clearance.

(D) The total number of security clearance periodic background investigations that were adjudicated with notice of a determination provided to the existing employee, including—

- (i) the total number of such adjudications that were adjudicated favorably; and
- (ii) the total number of such adjudications that were adjudicated unfavorably and resulted in a denial or revocation of a security clearance.

(E) The total number of pending security clearance background investigations, including initial applicant investigations and periodic reinvestigations, that were not adjudicated as of the last day of such year and that remained pending, categorized as follows:

- (i) For 180 days or shorter.
- (ii) For longer than 180 days, but shorter than 12 months.
- (iii) For 12 months or longer, but shorter than 18 months.
- (iv) For 18 months or longer, but shorter than 24 months.
- (v) For 24 months or longer.

(F) For any security clearance determinations completed or pending during the year preceding the year for which the report is submitted that have taken longer than 12 months to complete—

- (i) an explanation of the causes for the delays incurred during the period covered by the report; and
- (ii) the number of such delays involving a polygraph requirement.

(G) The percentage of security clearance investigations, including initial and periodic reinvestigations, that resulted in a denial or revocation of a security clearance.

(H) The percentage of security clearance investigations that resulted in incomplete information.

(I) The percentage of security clearance investigations that did not result in enough information to make a decision on potentially adverse information.

(3) The report required under this subsection shall be submitted in unclassified form, but may include a classified annex.

(c) FORM.—The reports required under subsections (a)(1) and (b) shall be submitted in unclassified form, but may include a classified annex.

**SUMMARY OF INTELLIGENCE RELATING TO TERRORIST RECIDIVISM OF
DETAINEES HELD AT UNITED STATES NAVAL STATION,
GUANTANAMO BAY, CUBA**

SEC. 506I. [50 U.S.C. § 3105]

(a) **IN GENERAL.**—The Director of National Intelligence, in consultation with the Director of the Central Intelligence Agency and the Director of the Defense Intelligence Agency, shall make publicly available an unclassified summary of—

(1) intelligence relating to recidivism of detainees currently or formerly held at the Naval Detention Facility at Guantanamo Bay, Cuba, by the Department of Defense; and

(2) an assessment of the likelihood that such detainees will engage in terrorism or communicate with persons in terrorist organizations.

(b) **UPDATES.**—Not less frequently than annually, the Director of National Intelligence, in consultation with the Director of the Central Intelligence Agency and the Secretary of Defense, shall update and make publicly available an unclassified summary consisting of the information required by subsection (a) and the number of individuals formerly detained at Naval Station, Guantanamo Bay, Cuba, who are confirmed or suspected of returning to terrorist activities after release or transfer from such Naval Station.

CLASSIFIED INTELLIGENCE BUDGET JUSTIFICATION MATERIALS

SEC 506J [50 U.S.C. § 3105a]

(a) **DEFINITIONS.**—In this section:

(1) **Budget.**—The term “budget” has the meaning given the term “budget of the President” in section 506A.

(2) **Classified intelligence budget justification materials.**— The term “classified intelligence budget justification materials” means, with respect to a fiscal year, the materials submitted to Congress by the Director of National Intelligence in support of the budget for that fiscal year that are classified or otherwise protected from public disclosure.

(b) **Timely Submission.**—Not later than 5 days after the date on which the President submits to Congress the budget for each fiscal year pursuant to section 1105(a) of title 31, United States Code, the Director of National Intelligence shall submit to the congressional intelligence committees the classified intelligence budget justification materials for the element for that budget.

**DATES OF SUBMITTAL OF VARIOUS ANNUAL AND SEMIANNUAL REPORTS
TO THE CONGRESSIONAL INTELLIGENCE COMMITTEES**

SEC. 507. [50 U.S.C. § 3106]

(a) **ANNUAL REPORTS.**—The date for the submittal to the congressional intelligence committees of the following annual reports shall be the date each year provided in subsection (c)(1):

(1) The annual report of the Inspectors General of the intelligence community on proposed resources and activities of their offices required by section 416(h) of title 5, United States Code.

(2) The annual report on certifications for immunity in interdiction of aircraft engaged in illicit drug trafficking required by section 1012(c)(2) of the National Defense Authorization Act for Fiscal Year 1995 (22 U.S.C. 2291-4(c)(2)).

(3) The annual report on activities under the David L. Boren National Security Education Act of 1991 (title VIII of Public Law 102-183; 50 U.S.C. 1901 et seq.) required by section 806(a) of that Act (50 U.S.C. 1906(a)).

(4) The annual report on hiring and retention of minority employees in the intelligence community required by section 114(a).

(5) The annual report on financial intelligence on terrorist assets required by section 118.

(6) An annual report submitted under section 119C(d)(1).

(b) **SEMIANNUAL REPORTS.**—The dates for the submittal to the congressional intelligence committees of the following semiannual reports shall be the dates each year provided in subsection (c)(2):

(1) The semiannual reports on decisions not to prosecute certain violations of law under the Classified Information Procedures Act (18 U.S.C. App.) as required by section 13 of that Act.

(2) The semiannual reports on the disclosure of information and consumer reports to the Federal Bureau of Investigation for counterintelligence purposes required by section 624(h)(2) of the Fair Credit Reporting Act (15 U.S.C. 1681u(h)(2)).

(3) The semiannual provision of information on requests for financial information for foreign counterintelligence purposes required by section 1114(a)(5)(C) of the Right to Financial Privacy Act of 1978 (12 U.S.C. 3414(a)(5)(C)).

(c) **SUBMITTAL DATES FOR REPORTS.**—

(1) Except as provided in subsection (d), each annual report listed in subsection (a) of this section shall be submitted not later than February 1.

(2) Except as provided in subsection (d), each semiannual report listed in subsection (b) shall be submitted not later than February 1 and August 1.

(d) POSTPONEMENT OF SUBMITTAL.—

(1) Subject to paragraph (3), the date for the submittal of—

(A) an annual report listed in subsection (a) may be postponed until March 1; and

(B) a semiannual report listed in subsection (b) may be postponed until March 1 or September 1, as the case may be, if the official required to submit such report submits to the congressional intelligence committees a written notification of such postponement.

(2)(A) Notwithstanding any other provision of law and subject to paragraph (3), the date for the submittal to the congressional intelligence committees of any report described in subparagraph (B) may be postponed by not more than 30 days from the date otherwise specified in the provision of law for the submittal of such report if the official required to submit such report submits to the congressional intelligence committees a written notification of such postponement.

(B) A report described in this subparagraph is any report on intelligence or intelligence-related activities of the United States Government that is submitted under a provision of law requiring the submittal of only a single report.

(3)(A) The date for the submittal of a report whose submittal is postponed under paragraph (1) or (2) may be postponed beyond the time provided for the submittal of such report under such paragraph if the official required to submit such report submits to the congressional intelligence committees a written certification that preparation and submittal of such report at such time will impede the work of officers or employees of the intelligence community in a manner that will be detrimental to the national security of the United States.

(B) A certification with respect to a report under subparagraph

(A) shall include a proposed submittal date for such report, and such report shall be submitted not later than that date.

CERTIFICATION OF COMPLIANCE WITH OVERSIGHT REQUIREMENTS

SEC. 508. [50 U.S.C. § 3107]

The head of each element of the intelligence community shall annually submit to the congressional intelligence committees—

(1) a certification that, to the best of the knowledge of the head of such element—

(A) the head of such element is in full compliance with the requirements of this title; and

- (B) any information required to be submitted by the head of such element under this Act before the date of the submission of such certification has been properly submitted; or
- (2) if the head of such element is unable to submit a certification under paragraph (1), a statement—
 - (A) of the reasons the head of such element is unable to submit such a certification;
 - (B) describing any information required to be submitted by the head of such element under this Act before the date of the submission of such statement that has not been properly submitted; and
 - (C) that the head of such element will submit such information as soon as possible after the submission of such statement.

AUDITABILITY OF CERTAIN ELEMENTS OF THE INTELLIGENCE COMMUNITY

SEC. 509. [50 U.S.C. § 3108]

(a) **REQUIREMENT FOR ANNUAL AUDITS.**—The head of each covered entity shall ensure that there is a full financial audit of such covered entity each year beginning with fiscal year 2014. Such audits may be conducted by an internal or external independent accounting or auditing organization.

(b) **REQUIREMENT FOR UNQUALIFIED OPINION.**—Beginning as early as practicable, but in no event later than the audit required under subsection (a) for fiscal year 2016, the head of each covered entity shall take all reasonable steps necessary to ensure that each audit required under subsection (a) contains an unqualified opinion on the financial statements of such covered entity for the fiscal year covered by such audit.

(c) **REPORTS TO CONGRESS.**—The chief financial officer of each covered entity shall provide to the congressional intelligence committees an annual audit report from an accounting or auditing organization on each audit of the covered entity conducted pursuant to subsection (a).

(d) **COVERED ENTITY DEFINED.**—In this section, the term “covered entity” means the Office of the Director of National Intelligence, the Central Intelligence Agency, the Defense Intelligence Agency, the National Security Agency, the National Reconnaissance Office, and the National Geospatial–Intelligence Agency.

**SIGNIFICANT INTERPRETATIONS OF LAW CONCERNING INTELLIGENCE
ACTIVITIES**

SEC. 510. [50 U.S.C. § 3109]

(a) NOTIFICATION.—Except as provided in subsection (c) and to the extent consistent with due regard for the protection from unauthorized disclosure of classified information relating to sensitive intelligence sources and methods or other exceptionally sensitive matters, the General Counsel of each element of the intelligence community shall notify the congressional intelligence committees, in writing, of any significant legal interpretation of the United States Constitution or Federal law affecting intelligence activities conducted by such element by not later than 30 days after the date of the commencement of any intelligence activity pursuant to such interpretation.

(b) CONTENT.—Each notification under subsection (a) shall provide a summary of the significant legal interpretation and the intelligence activity or activities conducted pursuant to such interpretation.

(c) EXCEPTIONS.—A notification under subsection (a) shall not be required for a significant legal interpretation if—

(1) notice of the significant legal interpretation was previously provided to the congressional intelligence committees under subsection (a); or

(2) the significant legal interpretation was made before July 7, 2014.

(d) LIMITED ACCESS FOR COVERT ACTION.—If the President determines that it is essential to limit access to a covert action finding under section 503(c)(2), the President may limit access to information concerning such finding that is subject to notification under this section to those members of Congress who have been granted access to the relevant finding under section 503(c)(2).

ANNUAL REPORT ON VIOLATIONS OF LAW OR EXECUTIVE ORDER

SEC. 511. [50 U.S.C. § 3110]

(a) ANNUAL REPORTS REQUIRED.—The Director of National Intelligence shall annually submit to the congressional intelligence committees a report on violations of law or executive order relating to intelligence activities by personnel of an element of the intelligence community that were identified during the previous calendar year.

(b) ELEMENTS.—Each report submitted under subsection (a) shall, consistent with the need to preserve ongoing criminal investigations, include a description of, and any action taken in response to, any violation of law or executive order (including Executive Order No. 12333 (50 U.S.C. 3001 note)) relating to intelligence activities committed by personnel of an element of the intelligence community in the course of the employment of such personnel that, during the previous calendar year, was—

- (1) determined by the director, head, or general counsel of any element of the intelligence community to have occurred;
- (2) referred to the Department of Justice for possible criminal prosecution; or
- (3) substantiated by the inspector general of any element of the intelligence community.

**BRIEFINGS AND NOTIFICATIONS ON COUNTERINTELLIGENCE ACTIVITIES OF
THE FEDERAL BUREAU OF INVESTIGATION**

SEC. 512. [50 U.S.C. § 3111]

(a) **QUARTERLY BRIEFINGS.**—In addition to, and without any derogation of, the requirement under section 501 to keep the congressional intelligence committees fully and currently informed of the intelligence and counterintelligence activities of the United States, not less frequently than once each quarter, or more frequently if requested by the congressional intelligence committees, the Director of the Federal Bureau of Investigation shall provide to the congressional intelligence committees a briefing on the counterintelligence activities of the Federal Bureau of Investigation. Such briefings shall include, at a minimum, an overview and updated of—

- (1) the counterintelligence posture of the Bureau;
- (2) counterintelligence investigations; and
- (3) any other information relating to the counterintelligence activities of the Bureau that the Director determines necessary.

(b) **NOTIFICATIONS.**—In addition to the quarterly briefings under subsection (a), the Director of the Federal Bureau of Investigation shall promptly notify the congressional intelligence committees of any counterintelligence investigation carried out by the Bureau with respect to any counterintelligence risk or threat that is related to an election or campaign for Federal office.

(c) **GUIDELINES.**—

(1) **DEVELOPMENT AND CONSULTATION.**—The Director shall develop guidelines governing the scope of the briefings provided under subsection (a), the notifications provided under subsection (b), and the information required by section 5304(a)(2) of the Damon Paul Nelson and Matthew Young Pollard Intelligence Authorization Act for Fiscal Years 2018, 2019, and 2020. The Director shall consult the congressional intelligence committees during such development.

(2) **SUBMISSION.**—The Director shall submit to the congressional intelligence committees—

- (A) the guidelines under paragraph (1) upon issuance; and
- (B) any updates to such guidelines by not later than 15 days after making such update.

**ANNUAL REPORTS ON THE DOMESTIC ACTIVITIES OF THE INTELLIGENCE
COMMUNITY**

SEC. 513 [50 U.S.C. § 3112]

- (a) **REPORTS.** —Not later than January 31 of each year, the Director of National Intelligence shall submit to the congressional intelligence committee a report—
- (1) identifying all domestic activities undertaken by each element of the intelligence community during the prior fiscal year; and
 - (2) for each activity identified under paragraph (1), a statement of the legal authority authorizing such activity to be undertaken.
- (b) **FORM.** —Each report under subsection (a) shall be submitted in unclassified form, but may include a classified annex.

**UNFUNDED PRIORITIES OF THE INTELLIGENCE COMMUNITY: ANNUAL
REPORT**

SEC. 514. [50 U.S.C. § 3113.]

(a) **ANNUAL REPORT.**—Not later than 10 days after the date on which the budget of the President for a fiscal year is submitted to Congress pursuant to section 1105 of title 31, United States Code, the head of each element of the intelligence community shall prepare and submit to the Director of National Intelligence, the congressional intelligence committees, the Subcommittee on Defense of the Committee on Appropriations of the Senate, and the Subcommittee on Defense of the Committee on Appropriations of the House of Representatives a report on the unfunded priorities of the programs under the jurisdiction of such head.

(b) **ELEMENTS.**—

- (1) **IN GENERAL.** —Each report under subsection (a) shall specify, for each unfunded priority covered by such report, the following:
- (A) A summary description of such priority, including the objectives to be achieved if such priority is funded (whether in whole or in part).
 - (B) Whether such priority will satisfy a covert action or support collection against requirements identified in the National Intelligence Priorities Framework of the Office of the Director of National Intelligence (or any successor mechanism established for the prioritization of programs and activities), including a description of such requirements and the related prioritization level.
 - (C) The additional amount of funds recommended in connection with the objectives under subparagraph (A).
 - (D) Budget information with respect to the unfunded priority, including—
 - (i) the appropriation account;

(ii) the expenditure center; and

(iii) the project and, if applicable, subproject.

(2) **PRIORITIZATION OF PRIORITIES.**—Each report shall present the unfunded priorities covered by such report in overall order of urgency of priority among unfunded priorities.

(c) **UNFUNDED PRIORITY DEFINED.** —In this section, the term 'unfunded priority', in the case of a fiscal year, means a program, activity, or mission requirement of an element of the intelligence community that—

(1) is not funded in the budget of the President for the fiscal year as submitted to Congress pursuant to section 1105 of title 31, United States Code;

(2) is necessary to fulfill a covert action or to satisfy an information requirement associated with the collection, analysis, or dissemination of intelligence that has been documented within the National Intelligence Priorities Framework; and

(3) would have been recommended for funding by the head of the element of the intelligence community if—

(A) additional resources had been available for the budget to fund the program, activity, or mission requirement; or

(B) the program, activity, or mission requirement has emerged since the budget was formulated."

SUBMISSION OF COVERED DOCUMENTS AND CLASSIFIED ANNEXES

SEC. 515. [50 U.S.C. § 3114]

(a) **COVERED DOCUMENT DEFINED.** —In this section, the term 'covered document' means any executive order, memorandum, or policy directive issued by the President, including national security Presidential memoranda and Presidential policy directives, or such successor memoranda and directives.

(b) **REQUIREMENT.** —Not later than 7 days after the date on which the President issues or amends a covered document, the President, acting through the Director of National Intelligence, shall submit to the congressional intelligence committees, the Subcommittee on Defense of the Committee on Appropriations of the Senate, and the Subcommittee on Defense of the Committee on Appropriations of the House of Representatives the covered document and any classified annex accompanying that document if such covered document or annex contains a direction to, establishes a requirement for, or includes a restriction on any element of the intelligence community.'

SUBMISSION OF LEGISLATIVE PROPOSALS

SEC. 516. [50 U.S.C. § 3115]

Not later than 45 days after the date on which the President submits to Congress the budget for each fiscal year pursuant to section 1105(a) of title 31, United States Code, the Director of National Intelligence shall submit to the congressional intelligence committees, the Committee on Appropriations of the Senate, and the Committee on Appropriations of the House of Representatives any legislative provisions that are proposed by the Director to be enacted as part of the annual intelligence authorization bill for that fiscal year.

**TITLE VI—PROTECTION OF CERTAIN NATIONAL
SECURITY INFORMATION**

**PROTECTION OF IDENTITIES OF CERTAIN UNITED STATES UNDERCOVER
INTELLIGENCE OFFICERS, AGENTS, INFORMANTS, AND SOURCES**

SEC. 601. [50 U.S.C. § 3121]

(a) DISCLOSURE OF INFORMATION BY PERSONS HAVING OR HAVING HAD ACCESS TO CLASSIFIED INFORMATION THAT IDENTIFIES COVERT AGENT.—Whoever, having or having had authorized access to classified information that identifies a covert agent, intentionally discloses any information identifying such covert agent to any individual not authorized to receive classified information, knowing that the information disclosed so identifies such covert agent and that the United States is taking affirmative measures to conceal such covert agent’s intelligence relationship to the United States, shall be fined under title 18, United States Code, or imprisoned not more than 15 years, or both.

(b) DISCLOSURE OF INFORMATION BY PERSONS WHO LEARN IDENTITY OF COVERT AGENTS AS RESULT OF HAVING ACCESS TO CLASSIFIED INFORMATION.—Whoever, as a result of having authorized access to classified information, learns the identity of a covert agent and intentionally discloses any information identifying such covert agent to any individual not authorized to receive classified information, knowing that the information disclosed so identifies such covert agent and that the United States is taking affirmative measures to conceal such covert agent’s intelligence relationship to the United States, shall be fined under title 18, United States Code, or imprisoned not more than 10 years, or both.

(c) DISCLOSURE OF INFORMATION BY PERSONS IN COURSE OF PATTERN OF ACTIVITIES INTENDED TO IDENTIFY AND EXPOSE COVERT AGENTS.—Whoever, in the course of a pattern of activities intended to identify and expose covert agents and with reason to believe that such activities would impair or impede the

NATIONAL SECURITY ACT OF 1947

foreign intelligence activities of the United States, discloses any information that identifies an individual as a covert agent to any individual not authorized to receive classified information, knowing that the information disclosed so identifies such individual and that the United States is taking affirmative measures to conceal such individual's classified intelligence relationship to the United States, shall be fined under title 18, United States Code, or imprisoned not more than three years, or both.

(d) IMPOSITION OF CONSECUTIVE SENTENCES.—A term of imprisonment imposed under this section shall be consecutive to any other sentence of imprisonment.

DEFENSES AND EXCEPTIONS

SEC. 602. [50 U.S.C. § 3122]

(a) DISCLOSURE BY UNITED STATES OF IDENTITY OF COVERT AGENT.—It is a defense to a prosecution under section 601 that before the commission of the offense with which the defendant is charged, the United States had publicly acknowledged or revealed the intelligence relationship to the United States of the individual the disclosure of whose intelligence relationship to the United States is the basis for the prosecution.

(b) CONSPIRACY, MISPRISION OF FELONY, AIDING AND ABETTING, ETC.—

(1) Subject to paragraph (2), no person other than a person committing an offense under section 601 shall be subject to prosecution under such section by virtue of section 2 or 4 of title 18, United States Code, or shall be subject to prosecution for conspiracy to commit an offense under such section.

(2) Paragraph (1) shall not apply (A) in the case of a person who acted in the course of a pattern of activities intended to identify and expose covert agents and with reason to believe that such activities would impair or impede the foreign intelligence activities of the United States, or (B) in the case of a person who has authorized access to classified information.

(c) DISCLOSURE TO SELECT CONGRESSIONAL COMMITTEES ON INTELLIGENCE.—It shall not be an offense under section 601 to transmit information described in such section directly to either congressional intelligence committee.

(d) DISCLOSURE BY AGENT OF OWN IDENTITY.—It shall not be an offense under section 601 for an individual to disclose information that solely identifies himself as a covert agent.

EXTRATERRITORIAL JURISDICTION

SEC. 603. [50 U.S.C. § 3124]

There is jurisdiction over an offense under section 601 committed outside the United States if the individual committing the offense is a citizen of the United States or an alien lawfully admitted to the United States for permanent residence (as defined in section 101(a)(20) of the Immigration and Nationality Act).

PROVIDING INFORMATION TO CONGRESS

SEC. 604. [50 U.S.C. § 3125]

Nothing in this title may be construed as authority to withhold information from the Congress or from a committee of either House of Congress.

DEFINITIONS

SEC. 605. [50 U.S.C. § 3126]

For the purposes of this title:

- (1) The term “classified information” means information or material designated and clearly marked or clearly represented, pursuant to the provisions of a statute or Executive order (or a regulation or order issued pursuant to a statute or Executive order), as requiring a specific degree of protection against unauthorized disclosure for reasons of national security.
- (2) The term “authorized”, when used with respect to access to classified information, means having authority, right, or permission pursuant to the provisions of a statute, Executive order, directive of the head of any department or agency engaged in foreign intelligence or counterintelligence activities, order of any United States court, or provisions of any Rule of the House of Representatives or resolution of the Senate which assigns responsibility within the respective House of Congress for the oversight of intelligence activities.
- (3) The term “disclose” means to communicate, provide, impart, transmit, transfer, convey, publish, or otherwise make available.
- (4) The term “covert agent” means—
 - (A) a present or retired officer or employee of an intelligence agency or a present or retired member of the Armed Forces assigned to duty with an intelligence agency whose identity as such an officer, employee, or member is classified information;
or
 - (B) a United States citizen whose intelligence relationship to the United States is classified information, and—
 - (i) who acts as an agent of, or informant or source of operational assistance to, an intelligence agency, or

(ii) who is at the time of the disclosure acting as an agent of, or informant to, the foreign counterintelligence or foreign counterterrorism components of the Federal Bureau of Investigation; or

(C) an individual, other than a United States citizen, whose past or present intelligence relationship to the United States is classified information and who is a present or former agent of, or a present or former informant or source of operational assistance to, an intelligence agency.

(5) The term “intelligence agency” means the elements of the intelligence community, as that term is defined in section 3(4) [50 U.S.C. § 3003(4)].

(6) The term “informant” means any individual who furnishes information to an intelligence agency in the course of a confidential relationship protecting the identity of such individual from public disclosure.

(7) The terms “officer” and “employee” have the meanings given such terms by section 2104 and 2105, respectively, of title 5, United States Code.

(8) The term “Armed Forces” means the Army, Navy, Air Force, Marine Corps, and Coast Guard.

(9) The term “United States”, when used in a geographic sense, means all areas under the territorial sovereignty of the United States and the Trust Territory of the Pacific Islands.

(10) The term “pattern of activities” requires a series of acts with a common purpose or objective.

TITLE VII—PROTECTION OF OPERATIONAL FILES

OPERATIONAL FILES OF THE CENTRAL INTELLIGENCE AGENCY

SEC. 701. [50 U.S.C. § 3141]

(a) The Director of the Central Intelligence Agency, with the coordination of the Director of National Intelligence, may exempt operational files of the Central Intelligence Agency from the provisions of section 552 of title 5, United States Code (Freedom of Information Act), which require publication or disclosure, or search or review in connection therewith.

(b) In this section, the term “operational files” means—

(1) files of the National Clandestine Service which document the conduct of foreign intelligence or counterintelligence operations or intelligence or security liaison arrangements or information exchanges with foreign governments or their intelligence or security services;

(2) files of the Directorate for Science and Technology which document the means by which foreign intelligence or counterintelligence is collected through scientific and technical systems; and

(3) files of the Office of Personnel Security which document investigations conducted to determine the suitability of potential foreign intelligence or counterintelligence sources; except that files which are the sole repository of disseminated intelligence are not operational files.

(c) Notwithstanding subsection (a), exempted operational files shall continue to be subject to search and review for information concerning—

(1) United States citizens or aliens lawfully admitted for permanent residence who have requested information on themselves pursuant to the provisions of section 552 of title 5, United States Code (Freedom of Information Act), or section 552a of title 5, United States Code (Privacy Act of 1974);

(2) any special activity the existence of which is not exempt from disclosure under the provisions of section 552 of title 5, United States Code (Freedom of Information Act); or

(3) the specific subject matter of an investigation by the congressional intelligence committees, the Intelligence Oversight Board, the Department of Justice, the Office of General Counsel of the Central Intelligence Agency, the Office of Inspector General of the Central Intelligence Agency, or the Office of the Director of National Intelligence for any impropriety, or violation of law, Executive order, or Presidential directive, in the conduct of an intelligence activity.

(d)(1) Files that are not exempted under subsection (a) of this section which contain information derived or disseminated from exempted operational files shall be subject to search and review.

(2) The inclusion of information from exempted operational files in files that are not exempted under subsection (a) of this section shall not affect the exemption under subsection (a) of this section of the originating operational files from search, review, publication, or disclosure.

(3) Records from exempted operational files which have been disseminated to and referenced in files that are not exempted under subsection (a) of this section and which have been returned to exempted operational files for sole retention shall be subject to search and review.

(e) The provisions of subsection (a) of this section shall not be superseded except by a provision of law which is enacted after the date of enactment of subsection (a), and which specifically cites and repeals or modifies its provisions.

(f) Whenever any person who has requested agency records under section 552 of title 5, United States Code (Freedom of Information Act), alleges that the Central Intelligence Agency has improperly withheld records because of failure to comply with any provision of this section, judicial review shall be available

under the terms set forth in section 552(a)(4)(B) of title 5, United States Code, except that—

(1) in any case in which information specifically authorized under criteria established by an Executive order to be kept secret in the interest of national defense or foreign relations which is filed with, or produced for, the court by the Central Intelligence Agency, such information shall be examined *ex parte*, *in camera* by the court;

(2) the court shall, to the fullest extent practicable, determine issues of fact based on sworn written submissions of the parties;

(3) when a complainant alleges that requested records are improperly withheld because of improper placement solely in exempted operational files, the complainant shall support such allegation with a sworn written submission, based upon personal knowledge or otherwise admissible evidence;

(4)(A) when a complainant alleges that requested records were improperly withheld because of improper exemption of operational files, the Central Intelligence Agency shall meet its burden under section 552(a)(4)(B) of title 5, United States Code, by demonstrating to the court by sworn written submission that exempted operational files likely to contain responsive records currently perform the functions set forth in subsection (b) of this section; and

(B) the court may not order the Central Intelligence Agency to review the content of any exempted operational file or files in order to make the demonstration required under subparagraph (A) of this paragraph, unless the complainant disputes the Central Intelligence Agency's showing with a sworn written submission based on personal knowledge or otherwise admissible evidence;

(5) in proceedings under paragraphs (3) and (4) of this subsection, the parties shall not obtain discovery pursuant to rules 26 through 36 of the Federal Rules of Civil Procedure, except that requests for admission may be made pursuant to rules 26 and 36;

(6) if the court finds under this subsection that the Central Intelligence Agency has improperly withheld requested records because of failure to comply with any provision of this section, the court shall order the Central Intelligence Agency to search and review the appropriate exempted operational file or files for the requested records and make such records, or portions thereof, available in accordance with the provisions of section 552 of title 5, United States Code (Freedom of Information Act), and such order shall be the exclusive remedy for failure to comply with this section; and

(7) if at any time following the filing of a complaint pursuant to this subsection the Central Intelligence Agency agrees to search the appropriate exempted operational file or files for the requested records, the court shall dismiss the claim based upon such complaint.

(g) DECENNIAL REVIEW OF EXEMPTED OPERATIONAL FILES.—

(1) Not less than once every ten years, the Director of the Central Intelligence Agency and the Director of National Intelligence shall review the exemptions in force under subsection (a) to determine whether such exemptions may be removed from any category of exempted files or any portion thereof.

(2) The review required by paragraph (1) shall include consideration of the historical value or other public interest in the subject matter of the particular category of files or portions thereof and the potential for declassifying a significant part of the information contained therein.

(3) A complainant who alleges that the Central Intelligence Agency has improperly withheld records because of failure to comply with this subsection may seek judicial review in the district court of the United States of the district in which any of the parties reside, or in the District of Columbia. In such a proceeding, the court's review shall be limited to determining the following:

(A) Whether the Central Intelligence Agency has conducted the review required by paragraph (1) before October 15, 1994, or before the expiration of the 10-year period beginning on the date of the most recent review.

(B) Whether the Central Intelligence Agency, in fact, considered the criteria set forth in paragraph (2) in conducting the required review.

**OPERATIONAL FILES OF THE NATIONAL GEOSPATIAL-INTELLIGENCE
AGENCY**

SEC. 702. [50 U.S.C. § 3142]

(a) EXEMPTION OF CERTAIN OPERATIONAL FILES FROM SEARCH, REVIEW, PUBLICATION, OR DISCLOSURE.—

(1) The Director of the National Geospatial-Intelligence Agency, with the coordination of the Director of National Intelligence, may exempt operational files of the National Geospatial-Intelligence Agency from the provisions of section 552 of title 5, United States Code, which require publication, disclosure, search, or review in connection therewith.

(2)(A) Subject to subparagraph (B), for the purposes of this section, the term "operational files" means files of the National Geospatial-Intelligence Agency (hereafter in this section referred to as "NGA")

concerning the activities of NGA that before the establishment of NGA were performed by the National Photographic Interpretation Center of the Central Intelligence Agency (NPIC), that document the means by which foreign intelligence or counterintelligence is collected through scientific and technical systems.

(B) Files which are the sole repository of disseminated intelligence are not operational files.

(3) Notwithstanding paragraph (1), exempted operational files shall continue to be subject to search and review for information concerning—

(A) United States citizens or aliens lawfully admitted for permanent residence who have requested information on themselves pursuant to the provisions of section 552 or 552a of title 5, United States Code;

(B) any special activity the existence of which is not exempt from disclosure under the provisions of section 552 of title 5, United States Code; or

(C) the specific subject matter of an investigation by any of the following for any impropriety, or violation of law, Executive order, or Presidential directive, in the conduct of an intelligence activity:

(i) The congressional intelligence committees.

(ii) The Intelligence Oversight Board.

(iii) The Department of Justice.

(iv) The Office of General Counsel of NGA.

(v) The Office of the Director of NGA.

(vi) The Office of the Inspector General of the National-Geospatial Intelligence Agency.

(4)(A) Files that are not exempted under paragraph (1) which contain information derived or disseminated from exempted operational files shall be subject to search and review.

(B) The inclusion of information from exempted operational files in files that are not exempted under paragraph (1) shall not affect the exemption under paragraph (1) of the originating operational files from search, review, publication, or disclosure.

(C) Records from exempted operational files which have been disseminated to and referenced in files that are not exempted under paragraph (1) and which have been returned to exempted operational files for sole retention shall be subject to search and review.

(5) The provisions of paragraph (1) may not be superseded except by a provision of law which is enacted after December 3, 1999, and which specifically cites and repeals or modifies its provisions.

(6)(A) Except as provided in subparagraph (B), whenever any person who has requested agency records under section 552 of title 5, United States Code, alleges that NGA has withheld records improperly because of failure to comply with any provision of this section, judicial review shall be available under the terms set forth in section 552(a)(4)(B) of title 5, United States Code.

(B) Judicial review shall not be available in the manner provided for under subparagraph (A) as follows:

(i) In any case in which information specifically authorized under criteria established by an Executive order to be kept secret in the interests of national defense or foreign relations is filed with, or produced for, the court by NGA, such information shall be examined *ex parte*, *in camera* by the court.

(ii) The court shall, to the fullest extent practicable, determine the issues of fact based on sworn written submissions of the parties.

(iii) When a complainant alleges that requested records are improperly withheld because of improper placement solely in exempted operational files, the complainant shall support such allegation with a sworn written submission based upon personal knowledge or otherwise admissible evidence.

(iv)(I) When a complainant alleges that requested records were improperly withheld because of improper exemption of operational files, NGA shall meet its burden under section 552(a)(4)(B) of title 5, United States Code, by demonstrating to the court by sworn written submission that exempted operational files likely to contain responsive records currently perform the functions set forth in paragraph (2).

(II) The court may not order NGA to review the content of any exempted operational file or files in order to make the demonstration required under subclause (I), unless the complainant disputes NGA's showing with a sworn written submission based on personal knowledge or otherwise admissible evidence.

(v) In proceedings under clauses (iii) and (iv), the parties may not obtain discovery pursuant to rules 26 through 36 of the Federal Rules of Civil Procedure, except that

requests for admissions may be made pursuant to rules 26 and 36.

(vi) If the court finds under this paragraph that NGA has improperly withheld requested records because of failure to comply with any provision of this subsection, the court shall order NGA to search and review the appropriate exempted operational file or files for the requested records and make such records, or portions thereof, available in accordance with the provisions of section 552 of title 5, United States Code, and such order shall be the exclusive remedy for failure to comply with this subsection.

(vii) If at any time following the filing of a complaint pursuant to this paragraph NGA agrees to search the appropriate exempted operational file or files for the requested records, the court shall dismiss the claim based upon such complaint.

(viii) Any information filed with, or produced for the court pursuant to clauses (i) and (iv) shall be coordinated with the Director of National Intelligence prior to submission to the court.

(b) DECENNIAL REVIEW OF EXEMPTED OPERATIONAL FILES.—

(1) Not less than once every 10 years, the Director of the National Geospatial-Intelligence Agency and the Director of National Intelligence shall review the exemptions in force under subsection (a)(1) to determine whether such exemptions may be removed from the category of exempted files or any portion thereof. The Director of National Intelligence must approve any determination to remove such exemptions.

(2) The review required by paragraph (1) shall include consideration of the historical value or other public interest in the subject matter of the particular category of files or portions thereof and the potential for declassifying a significant part of the information contained therein.

(3) A complainant that alleges that NGA has improperly withheld records because of failure to comply with this subsection may seek judicial review in the district court of the United States of the district in which any of the parties reside, or in the District of Columbia. In such a proceeding, the court's review shall be limited to determining the following:

(A) Whether NGA has conducted the review required by paragraph (1) before the expiration of the 10-year period beginning on December 3, 1999 or before the expiration of the 10-year period beginning on the date of the most recent review.

(B) Whether NGA, in fact, considered the criteria set forth in paragraph (2) in conducting the required review.

OPERATIONAL FILES OF THE NATIONAL RECONNAISSANCE OFFICE

SEC. 703. [50 U.S.C. § 3143]

(a) EXEMPTION OF CERTAIN OPERATIONAL FILES FROM SEARCH, REVIEW, PUBLICATION, OR DISCLOSURE.—

(1) The Director of the National Reconnaissance Office, with the coordination of the Director of National Intelligence, may exempt operational files of the National Reconnaissance Office from the provisions of section 552 of title 5, United States Code, which require publication, disclosure, search, or review in connection therewith.

(2)(A) Subject to subparagraph (B), for the purposes of this section, the term “operational files” means files of the National Reconnaissance Office (hereafter in this section referred to as “NRO”) that document the means by which foreign intelligence or counterintelligence is collected through scientific and technical systems.

(B) Files which are the sole repository of disseminated intelligence are not operational files.

(3) Notwithstanding paragraph (1), exempted operational files shall continue to be subject to search and review for information concerning—

(A) United States citizens or aliens lawfully admitted for permanent residence who have requested information on themselves pursuant to the provisions of section 552 or 552a of title 5, United States Code;

(B) any special activity the existence of which is not exempt from disclosure under the provisions of section 552 of title 5, United States Code; or

(C) the specific subject matter of an investigation by any of the following for any impropriety, or violation of law, Executive order, or Presidential directive, in the conduct of an intelligence activity:

(i) The Permanent Select Committee on Intelligence of the House of Representatives.

(ii) The Select Committee on Intelligence of the Senate.

(iii) The Intelligence Oversight Board.

(iv) The Department of Justice.

(v) The Office of General Counsel of NRO.

(vi) The Office of the Director of NRO.

(vii) The Office of the Inspector General of the NRO.

(4)(A) Files that are not exempted under paragraph (1) which contain information derived or disseminated from exempted operational files shall be subject to search and review.

(B) The inclusion of information from exempted operational files in files that are not exempted under paragraph (1) shall not affect the exemption under paragraph (1) of the originating operational files from search, review, publication, or disclosure.

(C) The declassification of some of the information contained in exempted operational files shall not affect the status of the operational file as being exempt from search, review, publication, or disclosure.

(D) Records from exempted operational files which have been disseminated to and referenced in files that are not exempted under paragraph (1) and which have been returned to exempted operational files for sole retention shall be subject to search and review.

(5) The provisions of paragraph (1) may not be superseded except by a provision of law which is enacted after November 27, 2002, and which specifically cites and repeals or modifies its provisions.

(6)(A) Except as provided in subparagraph (B), whenever any person who has requested agency records under section 552 of title 5, United States Code, alleges that NRO has withheld records improperly because of failure to comply with any provision of this section, judicial review shall be available under the terms set forth in section 552(a)(4)(B) of title 5, United States Code.

(B) Judicial review shall not be available in the manner provided for under subparagraph (A) as follows:

(i) In any case in which information specifically authorized under criteria established by an Executive order to be kept secret in the interests of national defense or foreign relations is filed with, or produced for, the court by NRO, such information shall be examined ex parte, in camera by the court.

(ii) The court shall, to the fullest extent practicable, determine the issues of fact based on sworn written submissions of the parties.

(iii) When a complainant alleges that requested records are improperly withheld because of improper placement solely in exempted operational files, the complainant shall support such allegation with a sworn written submission based upon personal knowledge or otherwise admissible evidence.

(iv)(I) When a complainant alleges that requested records were improperly withheld because of improper exemption of operational files, NRO shall meet its burden under section 552(a)(4)(B) of title 5, United States Code, by demonstrating to the court by sworn written submission that exempted operational files likely to contain responsive records currently perform the functions set forth in paragraph (2).

(II) The court may not order NRO to review the content of any exempted operational file or files in order to make the demonstration required under subclause (I), unless the complainant disputes NRO's showing with a sworn written submission based on personal knowledge or otherwise admissible evidence.

(v) In proceedings under clauses (iii) and (iv), the parties may not obtain discovery pursuant to rules 26 through 36 of the Federal Rules of Civil Procedure, except that requests for admissions may be made pursuant to rules 26 and 36.

(vi) If the court finds under this paragraph that NRO has improperly withheld requested records because of failure to comply with any provision of this subsection, the court shall order NRO to search and review the appropriate exempted operational file or files for the requested records and make such records, or portions thereof, available in accordance with the provisions of section 552 of title 5, United States Code, and such order shall be the exclusive remedy for failure to comply with this subsection.

(vii) If at any time following the filing of a complaint pursuant to this paragraph NRO agrees to search the appropriate exempted operational file or files for the requested records, the court shall dismiss the claim based upon such complaint.

(viii) Any information filed with, or produced for the court pursuant to clauses (i) and (iv) shall be coordinated with the Director of National Intelligence prior to submission to the court.

(b) DECENNIAL REVIEW OF EXEMPTED OPERATIONAL FILES.—

(1) Not less than once every 10 years, the Director of the National Reconnaissance Office and the Director of National Intelligence shall

review the exemptions in force under subsection (a)(1) to determine whether such exemptions may be removed from the category of exempted files or any portion thereof. The Director of National Intelligence must approve any determination to remove such exemptions.

(2) The review required by paragraph (1) shall include consideration of the historical value or other public interest in the subject matter of the particular category of files or portions thereof and the potential for declassifying a significant part of the information contained therein.

(3) A complainant that alleges that NRO has improperly withheld records because of failure to comply with this subsection may seek judicial review in the district court of the United States of the district in which any of the parties reside, or in the District of Columbia. In such a proceeding, the court's review shall be limited to determining the following:

- (A) Whether NRO has conducted the review required by paragraph (1) before the expiration of the 10-year period beginning on November 27, 2002 or before the expiration of the 10-year period beginning on the date of the most recent review.
- (B) Whether NRO, in fact, considered the criteria set forth in paragraph (2) in conducting the required review.

OPERATIONAL FILES OF THE NATIONAL SECURITY AGENCY

SEC. 704. [50 U.S.C. § 3144]

(a) EXEMPTION OF CERTAIN OPERATIONAL FILES FROM SEARCH, REVIEW, PUBLICATION, OR DISCLOSURE.—The Director of the National Security Agency, in coordination with the Director of National Intelligence, may exempt operational files of the National Security Agency from the provisions of section 552 of title 5, United States Code, which require publication, disclosure, search, or review in connection therewith.

(b) OPERATIONAL FILES DEFINED.—

(1) In this section, the term “operational files” means—

- (A) files of the Signals Intelligence Directorate of the National Security Agency (and any successor organization of that directorate) that document the means by which foreign intelligence or counterintelligence is collected through technical systems; and
- (B) files of the Research Associate Directorate of the National Security Agency (and any successor organization of that directorate) that document the means by which foreign intelligence or counterintelligence is collected through scientific and technical systems.

(2) Files that are the sole repository of disseminated intelligence, and files that have been accessioned into the National Security Agency Archives (or any successor organization) are not operational files.

(c) SEARCH AND REVIEW FOR INFORMATION.—Notwithstanding subsection (a), exempted operational files shall continue to be subject to search and review for information concerning any of the following:

(1) United States citizens or aliens lawfully admitted for permanent residence who have requested information on themselves pursuant to the provisions of section 552 or 552a of title 5, United States Code.

(2) Any special activity the existence of which is not exempt from disclosure under the provisions of section 552 of title 5, United States Code.

(3) The specific subject matter of an investigation by any of the following for any impropriety, or violation of law, Executive order, or Presidential directive, in the conduct of an intelligence activity:

(A) The Committee on Armed Services and the Permanent Select Committee on Intelligence of the House of Representatives.

(B) The Committee on Armed Services and the Select Committee on Intelligence of the Senate.

(C) The Intelligence Oversight Board.

(D) The Department of Justice.

(E) The Office of General Counsel of the National Security Agency.

(F) The Office of the Inspector General of the Department of Defense.

(G) The Office of the Director of the National Security Agency.

(H) The Office of the Inspector General of the National Security Agency.

(d) INFORMATION DERIVED OR DISSEMINATED FROM EXEMPTED OPERATIONAL FILES.—

(1) Files that are not exempted under subsection (a) that contain information derived or disseminated from exempted operational files shall be subject to search and review.

(2) The inclusion of information from exempted operational files in files that are not exempted under subsection (a) shall not affect the exemption under subsection (a) of the originating operational files from search, review, publication, or disclosure.

(3) The declassification of some of the information contained in exempted operational files shall not affect the status of the operational file as being exempt from search, review, publication, or disclosure.

(4) Records from exempted operational files that have been disseminated to and referenced in files that are not exempted under subsection (a) and that have been returned to exempted operational files for sole retention shall be subject to search and review.

(e) SUPERCEDEMENT OF OTHER LAWS.—The provisions of subsection (a) may not be superseded except by a provision of law that is enacted after November 24, 2003, and that specifically cites and repeals or modifies such provisions.

(f) ALLEGATION; IMPROPER WITHHOLDING OF RECORDS; JUDICIAL REVIEW.—

(1) Except as provided in paragraph (2), whenever any person who has requested agency records under section 552 of title 5, United States Code, alleges that the National Security Agency has withheld records improperly because of failure to comply with any provision of this section, judicial review shall be available under the terms set forth in section 552(a)(4)(B) of title 5, United States Code.

(2) Judicial review shall not be available in the manner provided for under paragraph (1) as follows:

(A) In any case in which information specifically authorized under criteria established by an Executive order to be kept secret in the interests of national defense or foreign relations is filed with, or produced for, the court by the National Security Agency, such information shall be examined *ex parte*, *in camera* by the court.

(B) The court shall determine, to the fullest extent practicable, the issues of fact based on sworn written submissions of the parties.

(C) When a complainant alleges that requested records are improperly withheld because of improper placement solely in exempted operational files, the complainant shall support such allegation with a sworn written submission based upon personal knowledge or otherwise admissible evidence.

(D)(i) When a complainant alleges that requested records were improperly withheld because of improper exemption of operational files, the National Security Agency shall meet its burden under section 552(a)(4)(B) of title 5, United States Code, by demonstrating to the court by sworn written submission that exempted operational files likely to contain responsive records currently perform the functions set forth in subsection (b) of this section.

(ii) The court may not order the National Security Agency to review the content of any exempted operational file or files in order to make the demonstration required under clause (i), unless the

complainant disputes the National Security Agency's showing with a sworn written submission based on personal knowledge or otherwise admissible evidence.

(E) In proceedings under subparagraphs (C) and (D), the parties may not obtain discovery pursuant to rules 26 through 36 of the Federal Rules of Civil Procedure, except that requests for admissions may be made pursuant to rules 26 and 36.

(F) If the court finds under this subsection that the National Security Agency has improperly withheld requested records because of failure to comply with any provision of this subsection, the court shall order the Agency to search and review the appropriate exempted operational file or files for the requested records and make such records, or portions thereof, available in accordance with the provisions of section 552 of title 5, United States Code, and such order shall be the exclusive remedy for failure to comply with this section (other than subsection (g)).

(G) If at any time following the filing of a complaint pursuant to this paragraph the National Security Agency agrees to search the appropriate exempted operational file or files for the requested records, the court shall dismiss the claim based upon such complaint.

(H) Any information filed with, or produced for the court pursuant to subparagraphs (A) and (D) shall be coordinated with the Director of National Intelligence before submission to the court.

(g) DECENNIAL REVIEW OF EXEMPTED OPERATIONAL FILES.—

(1) Not less than once every 10 years, the Director of the National Security Agency and the Director of National Intelligence shall review the exemptions in force under subsection (a) to determine whether such exemptions may be removed from a category of exempted files or any portion thereof. The Director of National Intelligence must approve any determination to remove such exemptions.

(2) The review required by paragraph (1) shall include consideration of the historical value or other public interest in the subject matter of a particular category of files or portions thereof and the potential for declassifying a significant part of the information contained therein.

(3) A complainant that alleges that the National Security Agency has improperly withheld records because of failure to comply with this subsection may seek judicial review in the district court of the United States of the district in which any of the parties reside, or in the District

of Columbia. In such a proceeding, the court's review shall be limited to determining the following:

(A) Whether the National Security Agency has conducted the review required by paragraph (1) before the expiration of the 10-year period beginning on November 24, 2003 or before the expiration of the 10-year period beginning on the date of the most recent review.

(B) Whether the National Security Agency, in fact, considered the criteria set forth in paragraph (2) in conducting the required review.

**PROTECTION OF CERTAIN FILES OF THE OFFICE OF THE DIRECTOR OF
NATIONAL INTELLIGENCE**

SEC. 706. [50 U.S.C. § 3146]

(a) INAPPLICABILITY OF FOIA TO EXEMPTED OPERATIONAL FILES PROVIDED TO ODNI.—

(1) Subject to paragraph (2), the provisions of section 552 of title 5, United States Code, that require search, review, publication, or disclosure of a record shall not apply to a record provided to the Office of the Director of National Intelligence by an element of the intelligence community from the exempted operational files of such element.

(2) Paragraph (1) shall not apply with respect to a record of the Office that—

(A) contains information derived or disseminated from an exempted operational file, unless such record is created by the Office for the sole purpose of organizing such exempted operational file for use by the Office;

(B) is disseminated by the Office to a person other than an officer, employee, or contractor of the Office; or

(C) is no longer designated as an exempted operational file in accordance with this title.

(b) EFFECT OF PROVIDING FILES TO ODNI.—Notwithstanding any other provision of this title, an exempted operational file that is provided to the Office by an element of the intelligence community shall not be subject to the provisions of section 552 of title 5, United States Code, that require search, review, publication, or disclosure of a record solely because such element provides such exempted operational file to the Office.

(c) SEARCH AND REVIEW FOR CERTAIN PURPOSES.—Notwithstanding subsection (a) or (b), an exempted operational file shall continue to be subject to search and review for information concerning any of the following:

(1) United States citizens or aliens lawfully admitted for permanent residence who have requested information on themselves pursuant to the provisions of section 552 or 552a of title 5, United States Code.

(2) Any special activity the existence of which is not exempt from disclosure under the provisions of section 552 of title 5, United States Code.

(3) The specific subject matter of an investigation for any impropriety or violation of law, Executive order, or Presidential directive, in the conduct of an intelligence activity by any of the following:

(A) The Select Committee on Intelligence of the Senate.

(B) The Permanent Select Committee on Intelligence of the House of Representatives.

(C) The Intelligence Oversight Board.

(D) The Department of Justice.

(E) The Office of the Director of National Intelligence.

(F) The Office of the Inspector General of the Intelligence Community.

(d) DECENNIAL REVIEW OF EXEMPTED OPERATIONAL FILES.—

(1) Not less than once every 10 years, the Director of National Intelligence shall review the exemptions in force under subsection (a) to determine whether such exemptions may be removed from any category of exempted files or any portion thereof.

(2) The review required by paragraph (1) shall include consideration of the historical value or other public interest in the subject matter of the particular category of files or portions thereof and the potential for declassifying a significant part of the information contained therein.

(3) A complainant that alleges that the Director of National Intelligence has improperly withheld records because of failure to comply with this subsection may seek judicial review in the district court of the United States of the district in which any of the parties reside, or in the District of Columbia. In such a proceeding, the court's review shall be limited to determining the following:

(A) Whether the Director has conducted the review required by paragraph (1) before the expiration of the 10-year period beginning on the date of the enactment of the Intelligence Authorization Act for Fiscal Year 2010, or before the expiration of the 10-year period beginning on the date of the most recent review.

(B) Whether the Director of National Intelligence, in fact, considered the criteria set forth in paragraph (2) in conducting the required review.

(e) SUPERSEDURE OF OTHER LAWS.—The provisions of this section may not be superseded except by a provision of law that is enacted after the date of the enactment of this section, and that specifically cites and repeals or modifies such provisions.

(f) ALLEGATION; IMPROPER WITHHOLDING OF RECORDS; JUDICIAL REVIEW.—

(1) Except as provided in paragraph (2), whenever any person who has requested agency records under section 552 of title 5, United States Code, alleges that the Office has withheld records improperly because of failure to comply with any provision of this section, judicial review shall be available under the terms set forth in section 552(a)(4)(B) of title 5, United States Code.

(2) Judicial review shall not be available in the manner provided for under paragraph (1) as follows:

(A) In any case in which information specifically authorized under criteria established by an Executive order to be kept secret in the interests of national defense or foreign relations is filed with, or produced for, the court by the Office, such information shall be examined *ex parte*, *in camera* by the court.

(B) The court shall determine, to the fullest extent practicable, the issues of fact based on sworn written submissions of the parties.

(C)(i) When a complainant alleges that requested records were improperly withheld because of improper exemption of operational files, the Office may meet the burden of the Office under section 552(a)(4)(B) of title 5, United States Code, by demonstrating to the court by sworn written submission that exempted files likely to contain responsive records are records provided to the Office by an element of the intelligence community from the exempted operational files of such element.

(ii) The court may not order the Office to review the content of any exempted file in order to make the demonstration required under clause (i), unless the complainant disputes the Office's showing with a sworn written submission based on personal knowledge or otherwise admissible evidence.

(D) In proceedings under subparagraph (C), a party may not obtain discovery pursuant to rules 26 through 36 of the Federal Rules of Civil Procedure, except that requests for admissions may be made pursuant to rules 26 and 36 of the Federal Rules of Civil Procedure.

(E) If the court finds under this subsection that the Office has improperly withheld requested records because of failure to

comply with any provision of this section, the court shall order the Office to search and review each appropriate exempted file for the requested records and make such records, or portions thereof, available in accordance with the provisions of section 552 of title 5, United States Code (commonly referred to as the Freedom of Information Act), and such order shall be the exclusive remedy for failure to comply with this section.

(F) If at any time following the filing of a complaint pursuant to this paragraph the Office agrees to search each appropriate exempted file for the requested records, the court shall dismiss the claim based upon such complaint.

(g) DEFINITIONS.—In this section:

(1) The term “exempted operational file” means a file of an element of the intelligence community that, in accordance with this title, is exempted from the provisions of section 552 of title 5, United States Code, that require search, review, publication, or disclosure of such file.

(2) Except as otherwise specifically provided, the term “Office” means the Office of the Director of National Intelligence.

TITLE VIII—ACCESS TO CLASSIFIED INFORMATION PROCEDURES

PROCEDURES

SEC. 801. [50 U.S.C. § 3161]

(a) Not later than 180 days after October 14, 1994, the President shall, by Executive order or regulation, establish procedures to govern access to classified information which shall be binding upon all departments, agencies, and offices of the executive branch of Government. Such procedures shall, at a minimum—

(1) provide that, except as may be permitted by the President, no employee in the executive branch of Government may be given access to classified information by any department, agency, or office of the executive branch of Government unless, based upon an appropriate background investigation, such access is determined to be clearly consistent with the national security interests of the United States;

(2) establish uniform minimum requirements governing the scope and frequency of background investigations and reinvestigations for all employees in the executive branch of Government who require access to classified information as part of their official responsibilities;

(3) provide that all employees in the executive branch of Government who require access to classified information shall be required as a

condition of such access to provide to the employing department or agency written consent which permits access by an authorized investigative agency to relevant financial records, other financial information, consumer reports, travel records, and computers used in the performance of Government duties, as determined by the President, in accordance with section 802 of this title, during the period of access to classified information and for a period of three years thereafter;

(4) provide that all employees in the executive branch of Government who require access to particularly sensitive classified information, as determined by the President, shall be required, as a condition of maintaining access to such information, to submit to the employing department or agency, during the period of such access, relevant information concerning their financial condition and foreign travel, as determined by the President, as may be necessary to ensure appropriate security; and

(5) establish uniform minimum standards to ensure that employees in the executive branch of Government whose access to classified information is being denied or terminated under this title are appropriately advised of the reasons for such denial or termination and are provided an adequate opportunity to respond to all adverse information which forms the basis for such denial or termination before final action by the department or agency concerned.

(b)(1) Subsection (a) shall not be deemed to limit or affect the responsibility and power of an agency head pursuant to other law or Executive order to deny or terminate access to classified information if the national security so requires. Such responsibility and power may be exercised only when the agency head determines that the procedures prescribed by subsection (a) cannot be invoked in a manner that is consistent with the national security.

(2) Upon the exercise of such responsibility, the agency head shall submit a report to the congressional intelligence committees.

REQUESTS BY AUTHORIZED INVESTIGATIVE AGENCIES

SEC. 802. [50 U.S.C. § 3162]

(a)(1) Any authorized investigative agency may request from any financial agency, financial institution, or holding company, or from any consumer reporting agency, such financial records, other financial information, and consumer reports as may be necessary in order to conduct any authorized law enforcement investigation, counterintelligence inquiry, or security determination. Any authorized investigative agency may also request records maintained by any commercial entity within the United States pertaining to travel by an employee in the executive branch of Government outside the United States.

- (2) Requests may be made under this section where—
- (A) the records sought pertain to a person who is or was an employee in the executive branch of Government required by the President in an Executive order or regulation, as a condition of access to classified information, to provide consent, during a background investigation and for such time as access to the information is maintained, and for a period of not more than three years thereafter, permitting access to financial records, other financial information, consumer reports, and travel records; and
 - (B)(i) there are reasonable grounds to believe, based on credible information, that the person is, or may be, disclosing classified information in an unauthorized manner to a foreign power or agent of a foreign power;
 - (ii) information the employing agency deems credible indicates the person has incurred excessive indebtedness or has acquired a level of affluence which cannot be explained by other information known to the agency; or
 - (iii) circumstances indicate the person had the capability and opportunity to disclose classified information which is known to have been lost or compromised to a foreign power or an agent of a foreign power.
- (3) Each such request—
- (A) shall be accompanied by a written certification signed by the department or agency head or deputy department or agency head concerned, or by a senior official designated for this purpose by the department or agency head concerned (whose rank shall be no lower than Assistant Secretary or Assistant Director), and shall certify that—
 - (i) the person concerned is or was an employee within the meaning of paragraph (2)(A);
 - (ii) the request is being made pursuant to an authorized inquiry or investigation and is authorized under this section; and
 - (iii) the records or information to be reviewed are records or information which the employee has previously agreed to make available to the authorized investigative agency for review;
 - (B) shall contain a copy of the agreement referred to in subparagraph (A)(iii);
 - (C) shall identify specifically or by category the records or information to be reviewed; and

(D) shall inform the recipient of the request of the prohibition described in subsection (b).

(b) PROHIBITION OF CERTAIN DISCLOSURE.—

(1) PROHIBITION.—

(A) IN GENERAL.—If a certification is issued under subparagraph (B) and notice of the right to judicial review under subsection (c) is provided, no governmental or private entity that receives a request under subsection (a), or officer, employee, or agent thereof, shall disclose to any person that an authorized investigative agency described in subsection (a) has sought or obtained access to information under subsection (a).

(B) CERTIFICATION.—The requirements of subparagraph (A) shall apply if the head of an authorized investigative agency described in subsection (a), or a designee, certifies that the absence of a prohibition of disclosure under this subsection may result in—

- (i) a danger to the national security of the United States;
- (ii) interference with a criminal, counterterrorism, or counterintelligence investigation;
- (iii) interference with diplomatic relations; or
- (iv) danger to the life or physical safety of any person.

(2) EXCEPTION.—

(A) IN GENERAL.—A governmental or private entity that receives a request under subsection (a), or officer, employee, or agent thereof, may disclose information otherwise subject to any applicable nondisclosure requirement to—

- (i) those persons to whom disclosure is necessary in order to comply with the request;
- (ii) an attorney in order to obtain legal advice or assistance regarding the request; or
- (iii) other persons as permitted by the head of the authorized investigative agency described in subsection (a) or a designee.

(B) APPLICATION.—A person to whom disclosure is made under subparagraph (A) shall be subject to the nondisclosure requirements applicable to a person to whom a request is issued under subsection (a) in the same manner as the person to whom the request is issued.

(C) NOTICE.—Any recipient that discloses to a person described in subparagraph (A) information otherwise subject to a nondisclosure requirement shall inform the person of the applicable nondisclosure requirement.

(D) IDENTIFICATION OF DISCLOSURE RECIPIENTS.—At the request of the head of an authorized investigative agency described in subsection (a), or a designee, any person making or intending to make a disclosure under clause (i) or (iii) of subparagraph (A) shall identify to the head of the authorized investigative agency or such designee the person to whom such disclosure will be made or to whom such disclosure was made prior to the request.

(c) JUDICIAL REVIEW.—

(1) IN GENERAL.—A request under subsection (a) or a nondisclosure requirement imposed in connection with such request under subsection (b) shall be subject to judicial review under section 3511 of title 18, United States Code.

(2) NOTICE.—A request under subsection (a) shall include notice of the availability of judicial review described in paragraph (1).

(d)(1) Notwithstanding any other provision of law (other than section 6103 of the Internal Revenue Code of 1986), an entity receiving a request for records or information under subsection (a) shall, if the request satisfies the requirements of this section, make available such records or information within 30 days for inspection or copying, as may be appropriate, by the agency requesting such records or information.

(2) Any entity (including any officer, employee, or agent thereof) that discloses records or information for inspection or copying pursuant to this section in good faith reliance upon the certifications made by an agency pursuant to this section shall not be liable for any such disclosure to any person under this title, the constitution of any State, or any law or regulation of any State or any political subdivision of any State.

(e) Any agency requesting records or information under this section may, subject to the availability of appropriations, reimburse a private entity for any cost reasonably incurred by such entity in responding to such request, including the cost of identifying, reproducing, or transporting records or other data.

(f) An agency receiving records or information pursuant to a request under this section may disseminate the records or information obtained pursuant to such request outside the agency only—

(1) to the agency employing the employee who is the subject of the records or information;

(2) to the Department of Justice for law enforcement or counterintelligence purposes; or

(3) with respect to dissemination to an agency of the United States, if such information is clearly relevant to the authorized responsibilities of such agency.

(g) Nothing in this section may be construed to affect the authority of an investigative agency to obtain information pursuant to the Right to Financial Privacy Act (12 U.S.C. 3401 et seq.) or the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.).

SECURITY EXECUTIVE AGENT

SEC. 803. [50 U.S.C. § 3162a]

(a) **IN GENERAL.**—The Director of National Intelligence, or such other officer of the United States as the President may designate, shall serve as the Security Executive Agent for all departments and agencies of the United States.

(b) **DUTIES.**—The duties of the Security Executive Agent are as follows:

- (1) To direct the oversight of investigations, reinvestigations, adjudications, and, as applicable, polygraphs for eligibility for access to classified information or eligibility to hold a sensitive position made by any Federal agency.
- (2) To review the national security background investigation and adjudication programs of Federal agencies to determine whether such programs are being implemented in accordance with this section.
- (3) To develop and issue uniform and consistent policies and procedures to ensure the effective, efficient, timely, and secure completion of investigations, polygraphs, and adjudications relating to determinations of eligibility for access to classified information or eligibility to hold a sensitive position.
- (4) Unless otherwise designated by law, to serve as the final authority to designate a Federal agency or agencies to conduct investigations of persons who are proposed for access to classified information or for eligibility to hold a sensitive position to ascertain whether such persons satisfy the criteria for obtaining and retaining access to classified information or eligibility to hold a sensitive position, as applicable.
- (5) Unless otherwise designated by law, to serve as the final authority to designate a Federal agency or agencies to determine eligibility for access to classified information or eligibility to hold a sensitive position in accordance with Executive Order No. 12968 (50 U.S.C. 3161 note; relating to access to classified information).
- (6) To review and approve the policies of the Federal agencies that ensure reciprocal recognition of eligibility for access to classified information or eligibility to hold a sensitive position among Federal agencies, and to act as the final authority to arbitrate and resolve disputes among such agencies involving the reciprocity of investigations and adjudications of eligibility.

(7) To execute all other duties assigned to the Security Executive Agent by law.

(c) AUTHORITIES.—The Security Executive Agent shall—

(1) issue guidelines and instructions to the heads of Federal agencies to ensure appropriate uniformity, centralization, efficiency, effectiveness, timeliness, and security in processes relating to determinations by such agencies of eligibility for access to classified information or eligibility to hold a sensitive position, including such matters as investigations, polygraphs, adjudications, and reciprocity;

(2) have the authority to grant exceptions to, or waivers of, national security investigative requirements, including issuing implementing or clarifying guidance, as necessary;

(3) have the authority to assign, in whole or in part, to the head of any Federal agency (solely or jointly) any of the duties of the Security Executive Agent described in subsection (b) or the authorities described in paragraphs (1) and (2), provided that the exercise of such assigned duties or authorities is subject to the oversight of the Security Executive Agent, including such terms and conditions (including approval by the Security Executive Agent) as the Security Executive Agent determines appropriate; and

(4) define and set standards for continuous vetting for continued access to classified information and for eligibility to hold a sensitive position.

EXCEPTIONS

SEC. 804. [50 U.S.C. § 3163]

Except as otherwise specifically provided, the provisions of this title shall not apply to the President and Vice President, Members of the Congress, Justices of the Supreme Court, and Federal judges appointed by the President.

DEFINITIONS

SEC. 805. [50 U.S.C. § 3164]

For purposes of this title—

(1) the term “authorized investigative agency” means an agency authorized by law or regulation to conduct a counterintelligence investigation or investigations of persons who are proposed for access to classified information to ascertain whether such persons satisfy the criteria for obtaining and retaining access to such information;

(2) the term “classified information” means any information that has been determined pursuant to Executive Order No. 12356 of April 2, 1982, or successor orders, or the Atomic Energy Act of 1954 [42 U.S.C.

§ 2011 et seq], to require protection against unauthorized disclosure and that is so designated;

(3) the term “consumer reporting agency” has the meaning given such term in section 603 of the Consumer Credit Protection Act (15 U.S.C. 1681a);

(4) the term “employee” includes any person who receives a salary or compensation of any kind from the United States Government, is a contractor of the United States Government or an employee thereof, is an unpaid consultant of the United States Government, or otherwise acts for or on behalf of the United States Government, except as otherwise determined by the President;

(5) the terms “financial agency” and “financial institution” have the meanings given to such terms in section 5312(a) of title 31, United States Code, and the term “holding company” has the meaning given to such term in section 1101(6) of the Right to Financial Privacy Act of 1978 (12 U.S.C. 3401);

(6) the terms “foreign power” and “agent of a foreign power” have the same meanings as set forth in subsections (a) and (b) of section 101, respectively, of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801);

(7) the term “State” means each of the several States of the United States, the District of Columbia, the Commonwealth of Puerto Rico, the Commonwealth of the Northern Mariana Islands, the United States Virgin Islands, Guam, American Samoa, the Republic of the Marshall Islands, the Federated States of Micronesia, and the Republic of Palau, and any other possession of the United States; and

(8) the term “computer” means any electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device and any data or other information stored or contained in such device.

TITLE IX—APPLICATION OF SANCTIONS LAWS TO INTELLIGENCE ACTIVITIES

STAY OF SANCTIONS

SEC. 901. [50 U.S.C. § 3171]

Notwithstanding any provision of law identified in section 904, the President may stay the imposition of an economic, cultural, diplomatic, or other sanction or related action by the United States Government concerning a foreign country,

NATIONAL SECURITY ACT OF 1947

organization, or person when the President determines and reports to Congress in accordance with section 903 that to proceed without delay would seriously risk the compromise of an ongoing criminal investigation directly related to the activities giving rise to the sanction or an intelligence source or method directly related to the activities giving rise to the sanction. Any such stay shall be effective for a period of time specified by the President, which period may not exceed 120 days, unless such period is extended in accordance with section 902.

EXTENSION OF STAY

SEC. 902. [50 U.S.C. § 3172]

Whenever the President determines and reports to Congress in accordance with section 903 that a stay of sanctions or related actions pursuant to section 901 has not afforded sufficient time to obviate the risk to an ongoing criminal investigation or to an intelligence source or method that gave rise to the stay, he may extend such stay for a period of time specified by the President, which period may not exceed 120 days. The authority of this section may be used to extend the period of a stay pursuant to section 901 for successive periods of not more than 120 days each.

REPORTS

SEC. 903. [50 U.S.C. § 3173]

Reports to Congress pursuant to sections 901 and 902 shall be submitted promptly upon determinations under this title. Such reports shall be submitted to the Committee on International Relations of the House of Representatives and the Committee on Foreign Relations of the Senate. With respect to determinations relating to intelligence sources and methods, reports shall also be submitted to the congressional intelligence committees. With respect to determinations relating to ongoing criminal investigations, reports shall also be submitted to the Committees on the Judiciary of the House of Representatives and the Senate.

LAWS SUBJECT TO STAY

SEC. 904. [50 U.S.C. § 3174]

The President may use the authority of sections 901 and 902 to stay the imposition of an economic, cultural, diplomatic, or other sanction or related action by the United States Government related to the proliferation of weapons of mass destruction, their delivery systems, or advanced conventional weapons otherwise required to be imposed by the Chemical and Biological Weapons Control and Warfare Elimination Act of 1991 (title III of Public Law 102–182)

[22 U.S.C. § 5601 et seq.]; the Nuclear Proliferation Prevention Act of 1994 (title VIII of Public Law 103–236); title XVII of the National Defense Authorization Act for Fiscal Year 1991 (Public Law 101–510) (relating to the nonproliferation of missile technology); the Iran-Iraq Arms Nonproliferation Act of 1992 (title XVI of Public Law 102–484); section 573 of the Foreign Operations, Export Financing Related Programs Appropriations Act, 1994 (Public Law 103–87); section 563 of the Foreign Operations, Export Financing Related Programs Appropriations Act, 1995 (Public Law 103–306); and comparable provisions.

TITLE X—EDUCATION IN SUPPORT OF NATIONAL INTELLIGENCE

SUBTITLE A – SCIENCE AND TECHNOLOGY

SCHOLARSHIPS AND WORK-STUDY FOR PURSUIT OF GRADUATE DEGREES IN SCIENCE AND TECHNOLOGY

SEC. 1001. [50 U.S.C. § 3191]

(a) PROGRAM AUTHORIZED.—The Director of National Intelligence may carry out a program to provide scholarships and work-study for individuals who are pursuing graduate degrees in fields of study in science and technology that are identified by the Director as appropriate to meet the future needs of the intelligence community for qualified scientists and engineers.

(b) ADMINISTRATION.—If the Director of National Intelligence carries out the program under subsection (a), the Director shall administer the program through the Office of the Director of National Intelligence.

(c) IDENTIFICATION OF FIELDS OF STUDY.—If the Director of National Intelligence carries out the program under subsection (a), the Director shall identify fields of study under subsection (a) in consultation with the other heads of the elements of the intelligence community.

(d) ELIGIBILITY FOR PARTICIPATION.—An individual eligible to participate in the program is any individual who—

(1) either—

(A) is an employee of the intelligence community; or

(B) meets criteria for eligibility for employment in the intelligence community that are established by the Director of National Intelligence;

(2) is accepted in a graduate degree program in a field of study in science or technology identified under subsection (a); and

(3) is eligible for a security clearance at the level of Secret or above.

(e) REGULATIONS.—If the Director of National Intelligence carries out the program under subsection (a), the Director shall prescribe regulations for purposes of the administration of this section.

FRAMEWORK FOR CROSS-DISCIPLINARY EDUCATION AND TRAINING

SEC. 1002. [50 U.S.C. § 3192]

The Director of National Intelligence shall establish an integrated framework that brings together the educational components of the intelligence community in order to promote a more effective and productive intelligence community through cross-disciplinary education and joint training.

SUBTITLE B – FOREIGN LANGUAGES PROGRAM

**PROGRAM ON ADVANCEMENT OF FOREIGN LANGUAGES
CRITICAL TO THE INTELLIGENCE COMMUNITY**

SEC. 1011. [50 U.S.C. § 3201]

(a) **IN GENERAL.**—The Secretary of Defense and the Director of National Intelligence may jointly carry out a program to advance skills in foreign languages that are critical to the capability of the intelligence community to carry out the national security activities of the United States (hereinafter in this subtitle referred to as the “Foreign Languages Program”).

(b) **IDENTIFICATION OF REQUISITE ACTIONS.**—In order to carry out the Foreign Languages Program, the Secretary of Defense and the Director of National Intelligence shall jointly identify actions required to improve the education of personnel in the intelligence community in foreign languages that are critical to the capability of the intelligence community to carry out the national security activities of the United States and to meet the long-term intelligence needs of the United States.

EDUCATION PARTNERSHIPS

SEC. 1012. [50 U.S.C. § 3202]

(a) **IN GENERAL.**—In carrying out the Foreign Languages Program, the head of a covered element of the intelligence community may enter into one or more education partnership agreements with educational institutions in the United States in order to encourage and enhance the study in such educational institutions of foreign languages that are critical to the capability of the intelligence community to carry out the national security activities of the United States.

(b) **ASSISTANCE PROVIDED UNDER EDUCATIONAL PARTNERSHIP AGREEMENTS.**—Under an educational partnership agreement entered into with an educational institution pursuant to this section, the head of a covered element of the intelligence community may provide the following assistance to the educational institution:

- (1) The loan of equipment and instructional materials of the element of the intelligence community to the educational institution for any purpose and duration that the head of the element considers appropriate.
- (2) Notwithstanding any other provision of law relating to the transfer of surplus property, the transfer to the educational institution of any computer equipment, or other equipment, that is—
 - (A) commonly used by educational institutions;
 - (B) surplus to the needs of the element of the intelligence community; and
 - (C) determined by the head of the element to be appropriate for support of such agreement.
- (3) The provision of dedicated personnel to the educational institution—
 - (A) to teach courses in foreign languages that are critical to the capability of the intelligence community to carry out the national security activities of the United States; or
 - (B) to assist in the development for the educational institution of courses and materials on such languages.
- (4) The involvement of faculty and students of the educational institution in research projects of the element of the intelligence community.
- (5) Cooperation with the educational institution in developing a program under which students receive academic credit at the educational institution for work on research projects of the element of the intelligence community.
- (6) The provision of academic and career advice and assistance to students of the educational institution.
- (7) The provision of cash awards and other items that the head of the element of the intelligence community considers appropriate.

VOLUNTARY SERVICES

SEC. 1013. [50 U.S.C. § 3203]

(a) **AUTHORITY TO ACCEPT SERVICES.**—Notwithstanding section 1342 of title 31, United States Code, and subject to subsection (b), the Foreign Languages Program under section 1011 shall include authority for the head of a covered element of the intelligence community to accept from any dedicated personnel voluntary services in support of the activities authorized by this subtitle.

(b) **REQUIREMENTS AND LIMITATIONS.**—

- (1) In accepting voluntary services from an individual under subsection (a), the head of a covered element of the intelligence community shall—
 - (A) supervise the individual to the same extent as the head of the element would supervise a compensated employee of that element providing similar services; and

(B) ensure that the individual is licensed, privileged, has appropriate educational or experiential credentials, or is otherwise qualified under applicable law or regulations to provide such services.

(2) In accepting voluntary services from an individual under subsection (a) of this section, the head of a covered element of the intelligence community may not—

(A) place the individual in a policymaking position, or other position performing inherently governmental functions; or

(B) compensate the individual for the provision of such services.

(c) **AUTHORITY TO RECRUIT AND TRAIN INDIVIDUALS PROVIDING SERVICES.**— The head of a covered element of the intelligence community may recruit and train individuals to provide voluntary services under subsection (a) of this section.

(d) **STATUS OF INDIVIDUALS PROVIDING SERVICES.**—

(1) Subject to paragraph (2), while providing voluntary services under subsection (a) of this section or receiving training under subsection (c) of this section, an individual shall be considered to be an employee of the Federal Government only for purposes of the following provisions of law:

(A) Section 552a of title 5, United States Code (relating to maintenance of records on individuals).

(B) Chapter 11 of title 18, United States Code (relating to conflicts of interest).

(2)(A) With respect to voluntary services under paragraph (1) provided by an individual that are within the scope of the services accepted under that paragraph, the individual shall be deemed to be a volunteer of a governmental entity or nonprofit institution for purposes of the Volunteer Protection Act of 1997 (42 U.S.C. 14501 et seq.).

(B) In the case of any claim against such an individual with respect to the provision of such services, section 4(d) of such Act (42 U.S.C. 14503(d)) shall not apply.

(3) Acceptance of voluntary services under this section shall have no bearing on the issuance or renewal of a security clearance.

(e) **REIMBURSEMENT OF INCIDENTAL EXPENSES.**—

(1) The head of a covered element of the intelligence community may reimburse an individual for incidental expenses incurred by the individual in providing voluntary services under subsection (a) of this section. The head of a covered element of the intelligence community shall determine which expenses are eligible for reimbursement under this subsection.

(2) Reimbursement under paragraph (1) may be made from appropriated or nonappropriated funds.

(f) **AUTHORITY TO INSTALL EQUIPMENT.**—

(1) The head of a covered element of the intelligence community may install telephone lines and any necessary telecommunication equipment in the private residences of individuals who provide voluntary services under subsection (a) of this section).

(2) The head of a covered element of the intelligence community may pay the charges incurred for the use of equipment installed under paragraph (1) for authorized purposes.

(3) Notwithstanding section 1348 of title 31, United States Code, the head of a covered element of the intelligence community may use appropriated funds or nonappropriated funds of the element in carrying out this subsection.

REGULATIONS

SEC. 1014. [50 U.S.C. § 3204]

(a) **IN GENERAL.**—The Secretary of Defense and the Director of National Intelligence shall jointly prescribe regulations to carry out the Foreign Languages Program.

(b) **ELEMENTS OF THE INTELLIGENCE COMMUNITY.**—The head of each covered element of the intelligence community shall prescribe regulations to carry out sections 1012 and 1013 with respect to that element including the following:

(1) Procedures to be utilized for the acceptance of voluntary services under section 1013.

(2) Procedures and requirements relating to the installation of equipment under section 1013(f).

DEFINITIONS

SEC. 1015. [50 U.S.C. § 3205]

In this subtitle:

(1) The term “covered element of the intelligence community” means an agency, office, bureau, or element referred to in subparagraphs (B) through (L) of section 3(4).

(2) The term “educational institution” means—

(A) a local educational agency (as that term is defined in section 8101 of the Elementary and Secondary Education Act of 1965);

(B) an institution of higher education (as defined in section 102 of the Higher Education Act of 1965 (20 U.S.C. 1002) other than

institutions referred to in subsection (a)(1)(C) of such section);
or

(C) any other nonprofit institution that provides instruction of foreign languages in languages that are critical to the capability of the intelligence community to carry out national security activities of the United States.

(3) The term “dedicated personnel” means employees of the intelligence community and private citizens (including former civilian employees of the Federal Government who have been voluntarily separated, and members of the United States Armed Forces who have been honorably discharged, honorably separated, or generally discharged under honorable circumstances and rehired on a voluntary basis specifically to perform the activities authorized under this subtitle).

SUBTITLE C – ADDITIONAL EDUCATION PROGRAMS

ASSIGNMENT OF INTELLIGENCE COMMUNITY PERSONNEL AS LANGUAGE STUDENTS

SEC. 1021. [50 U.S.C. § 3221]

(a) **IN GENERAL.**—The Director of National Intelligence, acting through the heads of the elements of the intelligence community, may assign employees of such elements in analyst positions requiring foreign language expertise as students at accredited professional, technical, or other institutions of higher education for training at the graduate or undergraduate level in foreign languages required for the conduct of duties and responsibilities of such positions.

(b) **AUTHORITY FOR REIMBURSEMENT OF COSTS OF TUITION AND TRAINING.**—

(1) The Director of National Intelligence may reimburse an employee assigned under subsection (a) for the total cost of the training described in that subsection, including costs of educational and supplementary reading materials.

(2) The authority under paragraph (1) shall apply to employees who are assigned on a full-time or part-time basis.

(3) Reimbursement under paragraph (1) may be made from appropriated or nonappropriated funds.

(c) **RELATIONSHIP TO COMPENSATION AS AN ANALYST.**—Reimbursement under this section to an employee who is an analyst is in addition to any benefits, allowances, travel expenses, or other compensation the employee is entitled to by reason of serving in such an analyst position.

PROGRAM ON RECRUITMENT AND TRAINING

SEC. 1022. [50 U.S.C. § 3222]

(a) PROGRAM.—

(1) REQUIREMENT. —The Director of National Intelligence, in consultation with the heads of the elements of the intelligence community, shall carry out a program to ensure that selected individuals are provided funds for academic training (including with respect to both undergraduate and postgraduate education), or to reimburse for academic training previously obtained—

(A) in capabilities, missions, or skillsets, especially in the fields of science, technology, math, and engineering, to address workforce requirements in which the intelligence community is deficient or likely to be deficient in the future; or

(B) for such individuals who have backgrounds or experiences that the Director has identified as—

(i) contributing to capabilities, missions, or skillsets in which the intelligence community is deficient or likely to be deficient in future; and

(ii) being underrepresented in the intelligence community or likely to be underrepresented in the future.

(2) COMMITMENT. —An individual selected for participation in the program shall commit to employment with an element of the intelligence community for a period that the Director determines is commensurate with the amount of funding provided to the individual under the program and under such terms and conditions as the Director considers appropriate.

(3) DESIGNATION. —The program shall be known as the Pat Roberts Intelligence Scholars Program.

(4) OUTREACH. —The Director, in consultation with the heads of the elements of the intelligence community, shall maintain a publicly available internet website on the program that describes—

(A) the intent of the program;

(B) the conditions and requirements for selection and participation;

(C) application instructions;

(D) the areas covered by the program pursuant to the review conducted under subsection (b)(2); and

(E) any other details the Director determines appropriate.

(b) ELEMENTS. —In carrying out the program under subsection (a), the Director shall—

- (1) establish such requirements relating to the academic training of participants as the Director considers appropriate to ensure that participants are prepared for employment as intelligence professionals; and
 - (2) on an annual basis, review the areas that will contribute to the capabilities, missions, and skillsets in which the intelligence community is deficient or is likely to be deficient in the future.
- (c) USE OF FUNDS. —Funds made available for the program under subsection (a) shall be used—
- (1) to provide a monthly stipend for each month that a participant is pursuing a course of study;
 - (2) to pay the partial or full tuition of a participant for the completion of such course of study;
 - (3) to reimburse a participant for tuition paid by the participant before becoming an employee of an element of the intelligence community, including with respect to providing payments for student loans used for such tuition;
 - (4) to pay for books and materials that the participant requires or required to complete such course of study;
 - (5) to pay the expenses of the participant for travel requested by an element of the intelligence community in relation to such program; or
 - (6) for such other purposes the Director considers reasonably appropriate to carry out such program.

EDUCATIONAL SCHOLARSHIP PROGRAM

SEC. 1023. [50 U.S.C. § 3223]

The head of a department or agency containing an element of the intelligence community may establish an undergraduate or graduate training program with respect to civilian employees and prospective civilian employees of such element similar in purpose, conditions, content, and administration to the program that the Secretary of Defense is authorized to establish under section 16 of the National Security Agency Act of 1959 [50 U.S.C. § 3614].

INTELLIGENCE OFFICER TRAINING PROGRAM

SEC. 1024. [50 U.S.C. § 3224]

(a) PROGRAMS.—

- (1) The Director of National Intelligence may carry out grant programs in accordance with subsections (b) and (c) to enhance the recruitment and retention of an ethnically and culturally diverse intelligence community workforce with capabilities critical to the national security interests of the United States.

(2) In carrying out paragraph (1), the Director shall identify the skills necessary to meet current or emergent needs of the intelligence community and the educational disciplines that will provide individuals with such skills.

(b) INSTITUTIONAL GRANT PROGRAM.—

(1) The Director may provide grants to institutions of higher education to support the establishment or continued development of programs of study in educational disciplines identified under subsection (a)(2).

(2) A grant provided under paragraph (1) may, with respect to the educational disciplines identified under subsection (a)(2), be used for the following purposes:

- (A) Curriculum or program development.
- (B) Faculty development.
- (C) Laboratory equipment or improvements.
- (D) Faculty research.

(c) GRANT PROGRAM FOR CERTAIN MINORITY-SERVING COLLEGES AND UNIVERSITIES.—

(1) The Director may provide grants to historically black colleges and universities and Predominantly Black Institutions, Hispanic Serving Institutions, and Asian American and Native American Pacific Islander-Serving Institutions to provide programs of study in educational disciplines identified under subsection (a)(2) or described in paragraph (2).

(2) A grant provided under paragraph (1) may be used to provide programs of study in the following educational disciplines:

- (A) Intermediate and advanced foreign languages deemed in the immediate interest of the intelligence community, including Farsi, Pashto, Middle Eastern, African, and South Asian dialects.
- (B) Study abroad programs and cultural immersion programs.

(d) APPLICATION.—An institution of higher education seeking a grant under this section shall submit an application describing the proposed use of the grant at such time and in such manner as the Director may require.

(e) REPORTS.—An institution of higher education that receives a grant under this section shall submit to the Director regular reports regarding the use of such grant, including—

- (1) a description of the benefits to students who participate in the course of study funded by such grant;
- (2) a description of the results and accomplishments related to such course of study; and
- (3) any other information that the Director may require.

(f) REGULATIONS.—The Director shall prescribe such regulations as may be necessary to carry out this section.

(g) DEFINITIONS.—In this section:

- (1) The term “Director” means the Director of National Intelligence.
- (2) HISTORICALLY BLACK COLLEGE AND UNIVERSITY.—The term “historically black college and university” has the meaning given the term “part B institution” in section 322 of the Higher Education Act of 1965 (20 U.S.C. 1061).
- (3) The term “institution of higher education” has the meaning given the term in section 101 of the Higher Education Act of 1965 (20 U.S.C. 1001).
- (4) PREDOMINANTLY BLACK INSTITUTION.—The term “Predominantly Black Institution” has the meaning given the term in section 318 of the Higher education [*sic*] Act of 1965 (20 U.S.C. 1059e).
- (5) HISPANIC-SERVING INSTITUTION.—The term “Hispanic-Serving Institution” has the meaning given the term in section 502(a)(5) of the Higher Education Act of 1965 (20 U.S.C. 1101a(a)(5)).
- (6) ASIAN AMERICAN AND NATIVE AMERICAN PACIFIC ISLANDER-SERVING INSTITUTION.—The term “Asian American and Native American Pacific Islander-Serving Institution” has the meaning given that term in section 320(b)(2) of the Higher Education Act of 1965 (20 U.S.C. 1059(g)(b)(2)).
- (7) STUDY ABROAD PROGRAM.—The term “study abroad program” means a program of study that—
 - (A) takes place outside the geographical boundaries of the United States;
 - (B) focuses on areas of the world that are critical to the national security interests of the United States and are generally underrepresented in study abroad programs at institutions of higher education, including Africa, Asia, Central and Eastern Europe, Eurasia, Latin America, and the Middle East; and
 - (C) is a credit or noncredit program.

**AUTHORIZATION OF SUPPORT BY DIRECTOR OF NATIONAL INTELLIGENCE
FOR CERTAIN WORKFORCE ACTIVITIES**

SEC. 1025 [50 U.S.C. § 3224a]

- (a) AUTHORIZATION.—The Director may, with or without reimbursement, obligate or expend amounts authorized to be appropriated or otherwise made available for the Office of the Director of National Intelligence for covered workforce activities for the purpose of supporting a covered workforce activity of an element of the intelligence community.
- (b) NOTIFICATION. —Not later than 30 days after the date on which the Director exercises the authority in subsection (a), the Director shall submit to the

congressional intelligence committees and the Committees on Appropriations of the House of Representatives and the Senate written notification of such exercise.

(c) **COVERED WORKFORCE ACTIVITY DEFINED.**—In this section, the term “covered workforce activity” means an activity relating to—

- (1) recruitment or retention of the intelligence community workforce; or
- (2) diversity, equality, inclusion, or accessibility, with respect to such workforce.

SUBTITLE D – NATIONAL INTELLIGENCE UNIVERSITY

TRANSFER DATE

SEC. 1031 [50 U.S.C. § 3227]

In this subtitle, the term ‘transfer date’ means the date on which the National Intelligence University is transferred from the Defense Intelligence Agency to the Director of National Intelligence under section 5324(a) of the National Defense Authorization Act for Fiscal Year 2020 (Public Law 116–92).

DEGREE-GRANTING AUTHORITY

SEC. 1032 [50 U.S.C. § 3227a]

(a) **IN GENERAL.**—Beginning on the transfer date, under regulations prescribed by the Director of National Intelligence, the President of the National Intelligence University may, upon the recommendation of the faculty of the University, confer appropriate degrees upon graduates who meet the degree requirements.

(b) **LIMITATION.**—A degree may not be conferred under this section unless—

- (1) the Secretary of Education has recommended approval of the degree in accordance with the Federal Policy Governing Granting of Academic Degrees by Federal Agencies; and
- (2) the University is accredited by the appropriate academic accrediting agency or organization to award the degree, as determined by the Secretary of Education.

REPORTING

SEC. 1033 [50 U.S.C. § 3227b]

(a) **IN GENERAL.**—Not less frequently than once each year, the Director of National Intelligence shall submit to the congressional intelligence committees a plan for employing professors, instructors, and lecturers at the National Intelligence University.

(b) **ELEMENTS.**—Each plan submitted under subsection (a) shall include the following:

NATIONAL SECURITY ACT OF 1947

(1) The total number of proposed personnel to be employed at the National Intelligence University.

(2) The total annual compensation to be provided the personnel described in paragraph (1).

(3) Such other matters as the Director considers appropriate.

(c) FORM OF SUBMITTAL.—Each plan submitted by the Director to the congressional intelligence committees under subsection (a) shall be submitted as part of another annual submission from the Director to the congressional intelligence committees.

NOTES

PLAN REGARDING PERSONNEL AT NATIONAL INTELLIGENCE UNIVERSITY.—

(1) INITIAL SUBMISSION.—Not later than 180 days after the date of the enactment of this Act, the Director of National Intelligence shall submit to the congressional intelligence committees the first submission required by section 1033(a) of the National Security Act of 1947, as added by subsection (a).

(2) CERTAIN REQUIREMENT NOT APPLICABLE.—Subsection (c) of section 1033 of the National Security Act of 1947, as added by subsection (a), shall not apply to the submittal under paragraph (1) of this subsection.

CONTINUED APPLICABILITY OF THE FEDERAL ADVISORY COMMITTEE ACT TO THE BOARD OF VISITORS

SEC. 1034 [50 U.S.C. § 3227c]

The Federal Advisory Committee Act (5 U.S.C. App.) shall continue to apply to the Board of Visitors of the National Intelligence University on and after the transfer date.

TITLE XI—ADDITIONAL MISCELLANEOUS PROVISIONS

APPLICABILITY TO UNITED STATES INTELLIGENCE ACTIVITIES OF FEDERAL LAWS IMPLEMENTING INTERNATIONAL TREATIES AND AGREEMENTS

SEC. 1101. [50 U.S.C. § 3231]

(a) IN GENERAL.—No Federal law enacted on or after December 27, 2000, that implements a treaty or other international agreement shall be construed as making unlawful an otherwise lawful and authorized intelligence activity of the United States Government or its employees, or any other person to the extent such other person is carrying out such activity on behalf of, and at the direction

of, the United States, unless such Federal law specifically addresses such intelligence activity.

(b) **AUTHORIZED INTELLIGENCE ACTIVITIES.**—An intelligence activity shall be treated as authorized for purposes of subsection (a) of this section if the intelligence activity is authorized by an appropriate official of the United States Government, acting within the scope of the official duties of that official and in compliance with Federal law and any applicable Presidential directive.

COUNTERINTELLIGENCE INITIATIVES

SEC. 1102. [50 U.S.C. § 3232]

(a) **INSPECTION PROCESS.**—In order to protect intelligence sources and methods from unauthorized disclosure, the Director of National Intelligence shall establish and implement an inspection process for all agencies and departments of the United States that handle classified information relating to the national security of the United States intended to assure that those agencies and departments maintain effective operational security practices and programs directed against counterintelligence activities.

(b) **ANNUAL REVIEW OF DISSEMINATION LISTS.**— The Director of National Intelligence shall establish and implement a process for all elements of the intelligence community to review, on an annual basis, individuals included on distribution lists for access to classified information. Such process shall ensure that only individuals who have a particularized “need to know” (as determined by the Director) are continued on such distribution lists.

(c) **COMPLETION OF FINANCIAL DISCLOSURE STATEMENTS REQUIRED FOR ACCESS TO CERTAIN CLASSIFIED INFORMATION.**—The Director of National Intelligence shall establish and implement a process by which each head of an element of the intelligence community directs that all employees of that element, in order to be granted access to classified information referred to in subsection (a) of section 1.3 of Executive Order No. 12968 (August 2, 1995; 60 Fed. Reg. 40245; [50 U.S.C. § 3161 note]), submit financial disclosure forms as required under subsection (b) of such section.

(d) **ARRANGEMENTS TO HANDLE SENSITIVE INFORMATION.**—The Director of National Intelligence shall establish, for all elements of the intelligence community, programs and procedures by which sensitive classified information relating to human intelligence is safeguarded against unauthorized disclosure by employees of those elements.

**MEASURES TO MITIGATE COUNTERINTELLIGENCE THREATS FROM
PROLIFERATION AND USE OF FOREIGN COMMERCIAL SPYWARE.**

SEC. 1102A. [50 U.S.C. §3232a]

(a) DEFINITIONS. —In this section:

(1) Appropriate congressional committees.—The term “appropriate congressional committees” means—

- (A) the Select Committee on Intelligence, the Committee on Foreign Relations, the Committee on Armed Services, the Committee on Banking, Housing, and Urban Affairs, the Committee on the Judiciary, the Committee on Appropriations, and the Committee on Homeland Security and Governmental Affairs of the Senate; and
- (B) the Permanent Select Committee on Intelligence, the Committee on Foreign Affairs, the Committee on Armed Services, the Committee on Financial Services, the Committee on the Judiciary, the Committee on Appropriations, the Committee on Homeland Security, and the Committee on Oversight and Reform of the House of Representatives.

(2) Covered entity.—The term “covered entity” means any foreign company that either directly or indirectly develops, maintains, owns, operates, brokers, markets, sells, leases, licenses, or otherwise makes available spyware.

(3) Foreign commercial spyware.—The term “foreign commercial spyware” means spyware that is developed (solely or in partnership with a foreign company), maintained, sold, leased, licensed, marketed, sourced (in whole or in part), or otherwise provided, either directly or indirectly, by a foreign company.

(4) Foreign company.—The term “foreign company” means a company that is incorporated or domiciled outside of the United States, including any subsidiaries or affiliates wherever such subsidiaries or affiliates are domiciled or incorporated.

(5) Spyware.—The term “spyware” means a tool or set of tools that operate as an end-to-end system of software to provide an unauthorized user remote access to information stored on or transiting through an electronic device connected to the Internet and not owned or operated by the unauthorized user, including end- to-end systems that—

- (A) allow an unauthorized user to remotely infect electronic devices with malicious software, including without any action required by the user of the device;
- (B) can record telecommunications or other audio captured on a device not owned by the unauthorized user;

(C) undertake geolocation, collect cell site location information, or otherwise track the location of a device or person using the internal sensors of an electronic device not owned by the unauthorized user;

(D) allow an unauthorized user access to and the ability to retrieve information on the electronic device, including text messages, files, e-mails, transcripts of chats, contacts, photos, and browsing history;

or

(E) any additional criteria described in publicly available documents published by the Director of National Intelligence, such as whether the end-to-end system is used outside the context of a codified lawful intercept system.

(b) ANNUAL ASSESSMENTS OF COUNTERINTELLIGENCE THREATS.—

(1) REQUIREMENT.—Not later than 90 days after the enactment of the Intelligence Authorization Act for Fiscal Year 2023, and annually thereafter, the Director of National Intelligence, in coordination with the Director of the Central Intelligence Agency, the Director of the National Security Agency, and the Director of the Federal Bureau of Investigation, shall submit to the appropriate congressional committees a report with an accompanying classified annex containing an assessment of the counterintelligence threats and other risks to the national security of the United States posed by the proliferation of foreign commercial spyware. The assessment shall incorporate all credible data, including open-source information.

(2) ELEMENTS.—Each report under paragraph (1) shall include the following, if known:

(A) A list of the most significant covered entities.

(B) A description of the foreign commercial spyware marketed by the covered entities identified under subparagraph (A) and an assessment by the intelligence community of the foreign commercial spyware.

(C) An assessment of the counterintelligence risk to the intelligence community or personnel of the intelligence community posed by foreign commercial spyware.

(D) For each covered entity identified in subparagraph (A), details of any subsidiaries, resellers, or other agents acting on behalf of the covered entity.

(E) Details of where each covered entity identified under subparagraphs (A) and (D) is domiciled.

(F) A description of how each covered entity identified under subparagraphs (A) and (D) is financed, where the covered entity acquired its capital, and the organizations and individuals having substantial investments or other equities in the covered entity.

(G) An assessment by the intelligence community of any relationship between each covered entity identified in subparagraphs (A) and (D) and any foreign government, including any export controls and processes to which the covered entity is subject.

(H) A list of the foreign customers of each covered entity identified in subparagraphs (A) and (D), including the understanding by the intelligence community of the organizations and end-users within any foreign government.

(I) With respect to each foreign customer identified under subparagraph (H), an assessment by the intelligence community regarding how the foreign customer is using the spyware, including whether the foreign customer has targeted personnel of the intelligence community.

(J) With respect to the first report required under paragraph (1), a mitigation plan to reduce the exposure of personnel of the intelligence community to foreign commercial spyware.

(K) With respect to each report following the first report required under paragraph (1), details of steps taken by the intelligence community since the previous report to implement measures to reduce the exposure of personnel of the intelligence community to foreign commercial spyware.

(3) CLASSIFIED ANNEX.—In submitting the report under paragraph (1), the Director shall also include an accompanying but separate classified annex, providing a watchlist of companies selling, leasing, or otherwise providing foreign commercial spyware that the Director determines are engaged in activities that pose a counterintelligence risk to personnel of the intelligence community.

(4) FORM.—Each report under paragraph (1) shall be submitted in classified form.

(5) DISSEMINATION.—The Director of National Intelligence shall separately distribute each report under paragraph (1) and each annex under paragraph (3) to the President, the heads of all elements of the intelligence community, the Secretary of State, the Attorney General, the Secretary of Commerce, the Secretary of Homeland Security, the National Cyber Director, and the heads of any other departments or agencies the Director of National Intelligence determines appropriate.

(c) AUTHORITY TO PROHIBIT PURCHASE OR USE BY INTELLIGENCE COMMUNITY.—

(1) FOREIGN COMMERCIAL SPYWARE.—

(A) In general.—The Director of National Intelligence may prohibit any element of the intelligence community from procuring, leasing, or otherwise acquiring on the commercial market, or extending or

renewing a contract to procure, lease, or otherwise acquire, foreign commercial spyware.

(B) CONSIDERATIONS.—In determining whether and how to exercise the authority under subparagraph (A), the Director of National Intelligence shall consider—

(i) the assessment of the intelligence community of the counterintelligence threats or other risks to the United States posed by foreign commercial spyware;

(ii) the assessment of the intelligence community of whether the foreign commercial spyware has been used to target United States Government personnel.

(iii) whether the original owner or developer retains any of the physical property or intellectual property associated with the foreign commercial spyware;

(iv) whether the original owner or developer has verifiably destroyed all copies of the data collected by or associated with the foreign commercial spyware;

(v) whether the personnel of the original owner or developer retain any access to data collected by or associated with the foreign commercial spyware;

(vi) whether the use of the foreign commercial spyware requires the user to connect to an information system of the original owner or developer or information system of a foreign government; and

(vii) whether the foreign commercial spyware poses a counterintelligence risk to the United States or any other threat to the national security of the United States.

(2) COMPANY THAT HAS ACQUIRED FOREIGN COMMERCIAL SPYWARE.—

(A) AUTHORITY.—The Director of National Intelligence may prohibit any element of the intelligence community from entering into any contract or other agreement for any purpose with a company that has acquired, in whole or in part, any foreign commercial spyware.

(B) CONSIDERATIONS.—In considering whether and how to exercise the authority under subparagraph (A), the Director of National Intelligence shall consider—

(i) whether the original owner or developer of the foreign commercial spyware retains any of the physical property or intellectual property associated with the spyware;

(ii) whether the original owner or developer of the foreign commercial spyware has verifiably destroyed all data, and any copies thereof, collected by or associated with the spyware;

- (iii) whether the personnel of the original owner or developer of the foreign commercial spyware retain any access to data collected by or associated with the foreign commercial spyware;
- (iv) whether the use of the foreign commercial spyware requires the user to connect to an information system of the original owner or developer or information system of a foreign government; and
- (v) whether the foreign commercial spyware poses a counterintelligence risk to the United States or any other threat to the national security of the United States.

(3) NOTIFICATIONS OF PROHIBITION.—Not later than 30 days after the date on which the Director of National Intelligence exercises the authority to issue a prohibition under subsection (c), the Director of National Intelligence shall notify the congressional intelligence committees of such exercise of authority. Such notice shall include—

- (A) a description of the circumstances under which the prohibition was issued;
- (B) an identification of the company or product covered by the prohibition;
- (C) any information that contributed to the decision of the Director of National Intelligence to exercise the authority, including any information relating to counterintelligence or other risks to the national security of the United States posed by the company or product, as assessed by the intelligence community; and
- (D) an identification of each element of the intelligence community to which the prohibition has been applied.

(4) WAIVER AUTHORITY.—

(A) IN GENERAL.—The head of an element of the intelligence community may request from the Director of National Intelligence the waiver of a prohibition made under paragraph (1) or (2).

(B) DIRECTOR OF NATIONAL INTELLIGENCE DETERMINATION.—The Director of National Intelligence, upon receiving the waiver request in subparagraph (A), may issue a waiver for a period not to exceed one year in response to the request from the head of an element of the intelligence community if such waiver is in the national security interest of the United States.

(C) NOTICE.—Not later than 30 days after approving a waiver request pursuant to subparagraph (B), the Director of National Intelligence shall submit to the congressional intelligence committees, the Subcommittee on Defense of the Committee on Appropriations of the Senate, and the Subcommittee on Defense of the Committee on Appropriations of the House of Representatives a written notification. The notification shall include—

- (i) an identification of the head of the element of the intelligence community that requested the waiver;
- (ii) the details of the waiver request, including the national security interests of the United States;
- (iii) the rationale and basis for the determination that the waiver is in the national security interests of the United States;
- (iv) the considerations that informed the ultimate determination of the Director of National Intelligence to issue the waiver; and
- (v) and any other considerations contributing to the determination, made by the Director of National Intelligence.

(D) **WAIVER TERMINATION.**—The Director of National Intelligence may revoke a previously granted waiver at any time. Upon revocation of a waiver, the Director of National Intelligence shall submit a written notification to the congressional intelligence committees, the Subcommittee on Defense of the Committee on Appropriations of the Senate, and the Subcommittee on Defense of the Committee on Appropriations of the House of Representatives not later than 30 days after making a revocation determination.

(5) **TERMINATION OF PROHIBITION.**—The Director of National Intelligence may terminate a prohibition made under paragraph (1) or (2) at any time. Upon termination of a prohibition, the Director of National Intelligence shall submit a notification of the termination to the congressional intelligence committees, the Subcommittee on Defense of the Committee on Appropriations of the Senate, and the Subcommittee on Defense of the Committee on Appropriations of the House of Representatives not later than 30 days after terminating a prohibition, detailing the basis for the termination, including any United States national security interests that may be affected by such termination.

MISUSE OF THE OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE NAME, INITIALS, OR SEAL

SEC. 1103. [50 U.S.C. § 3233]

(a) **PROHIBITED ACTS.**—No person may, except with the written permission of the Director of National Intelligence, or a designee of the Director, knowingly use the words “Office of the Director of National Intelligence”, the initials “ODNI”, the seal of the Office of the Director of National Intelligence, or any colorable imitation of such words, initials, or seal in connection with any merchandise, impersonation, solicitation, or commercial activity in a manner reasonably calculated to convey the impression that such use is approved, endorsed, or authorized by the Director of National Intelligence.

(b) INJUNCTION.—Whenever it appears to the Attorney General that any person is engaged or is about to engage in an act or practice which constitutes or will constitute conduct prohibited by subsection (a), the Attorney General may initiate a civil proceeding in a district court of the United States to enjoin such act or practice. Such court shall proceed as soon as practicable to the hearing and determination of such action and may, at any time before final determination, enter such restraining orders or prohibitions, or take such other action as is warranted, to prevent injury to the United States or to any person or class of persons for whose protection the action is brought.

PROHIBITED PERSONNEL PRACTICES IN THE INTELLIGENCE COMMUNITY

SEC. 1104. [50 U.S.C. § 3234]

(a) DEFINITIONS.—In this section:

(1) AGENCY.—The term “agency” means an executive department or independent establishment, as defined under sections 101 and 104 of title 5, United States Code, that contains an intelligence community element, except the Federal Bureau of Investigation.

(2) COVERED INTELLIGENCE COMMUNITY ELEMENT.—The term “covered intelligence community element”—

(A) means—

(i) the Central Intelligence Agency, the Defense Intelligence Agency, the National Geospatial-Intelligence Agency, the National Security Agency, the Office of the Director of National Intelligence, and the National Reconnaissance Office; and

(ii) any executive agency or unit thereof determined by the President under section 2302(a)(2)(C)(ii) of title 5, United States Code, to have as its principal function the conduct of foreign intelligence or counterintelligence activities; and

(B) does not include the Federal Bureau of Investigation.

(3) PERSONNEL ACTION.—The term “personnel action” means, with respect to an employee in a position in a covered intelligence community element (other than a position excepted from the competitive service due to its confidential, policy-determining, policymaking, or policy-advocating character) or a contractor employee—

(A) an appointment;

(B) a promotion;

(C) a disciplinary or corrective action;

(D) a detail, transfer, or reassignment;

(E) a demotion, suspension, or termination;

- (F) a reinstatement or restoration;
- (G) a performance evaluation;
- (H) a decision concerning pay, benefits, or awards;
- (I) a decision concerning education or training if such education or training may reasonably be expected to lead to an appointment, promotion, or performance evaluation; or
- (J) any other significant change in duties, responsibilities, or working conditions.

(4) **CONTRACTOR EMPLOYEE.**—The term “contractor employee” means an employee of a contractor, subcontractor, grantee, subgrantee, or personal services contractor, of a covered intelligence community element.

(b) **AGENCY EMPLOYEES.**—Any employee of a covered intelligence element or an agency who has authority to take, direct others to take, recommend, or approve any personnel action, shall not, with respect to such authority, take or fail to take, or threaten to take or fail to take, a personnel action with respect to any employee of a covered intelligence community element as a reprisal for—

(1) any lawful disclosure of information by the employee to the Director of National Intelligence (or an employee designated by the Director of National Intelligence for such purpose), the Inspector General of the Intelligence Community, a supervisor in the employee’s direct chain of command, or a supervisor of the employing agency with responsibility for the subject matter of the disclosure, up to and including, the head of the employing agency (or an employee designated by the head of that agency for such purpose), the appropriate inspector general of the employing agency, a congressional intelligence committee, or a member of a congressional intelligence committee, which the employee reasonably believes evidences—

- (A) a violation of any Federal law, rule, or regulation; or
- (B) mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety;

(2) any lawful disclosure that complies with—

- (A) subsections (a)(1), (d), and (g) of Section 8H of the Inspector General Act of 1978 (5 U.S.C. App.);
 - (B) subparagraphs (A), (D), and (H) of section 17(d)(5) of the Central Intelligence Agency Act of 1949 (50 U.S.C. 3517(d)(5));
- or

(C) subparagraphs (A), (D), and (I) of section 103H(k)(5); or

(3) if the actions do not result in the employee unlawfully disclosing information specifically required by Executive order to be kept classified

in the interest of national defense or the conduct of foreign affairs, any lawful disclosure in conjunction with—

- (A) the exercise of any appeal, complaint, or grievance right granted by any law, rule, or regulation;
- (B) testimony for or otherwise lawfully assisting any individual in the exercise of any right referred to in subparagraph (A); or
- (C) cooperation with or disclosing information to the Inspector General of an agency, in accordance with applicable provisions of law in connection with an audit, inspection, or investigation conducted by the Inspector General.

(c) CONTRACTOR EMPLOYEES.—

(1) Any employee of an agency or of a contractor, subcontractor, grantee, subgrantee, or personal services contractor, of a covered intelligence community element who has authority to take, direct others to take, recommend, or approve any personnel action, shall not, with respect to such authority, take or fail to take, or threaten to take or fail to take, a personnel action with respect to any contractor employee as a reprisal for

(A) any lawful disclosure of information by the contractor employee to the Director of National Intelligence (or an employee designated by the Director of National Intelligence for such purpose), the Inspector General of the Intelligence Community, a supervisor in the contractor employee's direct chain of command, or a supervisor of the employing or contracting agency with responsibility for the subject matter of the disclosure, up to and including, the head of the employing or contracting agency (or an employee designated by the head of that agency for that purpose) or employing contractor, the appropriate inspector general of the employing or contracting agency, a congressional intelligence committee, or a member of a congressional intelligence committee, which the contractor employee reasonably believes evidences—

- (i) a violation of any Federal law, rule, or regulation (including with respect to evidence of another employee or contractor employee accessing or sharing classified information without authorization); or
- (ii) mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety.

(B) any lawful disclosure that complies with—

- (i) subsections (a)(1), (d), and (g) of section 8H of the Inspector General Act of 1978 (5 U.S.C. App.);

- (ii) subparagraphs (A), (D), and (H) of section 3517(d)(5) of this title; or
- (iii) subparagraphs (A), (D), and (I) of section 3033(k)(5) of this title; or

(C) if the actions do not result in the contractor employee unlawfully disclosing information specifically required by Executive order to be kept classified in the interest of national defense or the conduct of foreign affairs, any lawful disclosure in conjunction with—

- (i) the exercise of any appeal, complaint, or grievance right granted by any law, rule, or regulation;
- (ii) testimony for or otherwise lawfully assisting any individual in the exercise of any right referred to in clause (i); or
- (iii) cooperation with or disclosing information to the Inspector General of an agency, in accordance with applicable provisions of law in connection with an audit, inspection, or investigation conducted by the Inspector General.

(2) A personnel action under paragraph (1) is prohibited even if the action is undertaken at the request of an agency official, unless the request takes the form of a nondiscretionary directive and is within the authority of the agency official making the request.

(d) **RULE OF CONSTRUCTION.** —Consistent with the protection of intelligence sources and methods, nothing in subsection (b) or (c) shall be construed to authorize—

- (1) the withholding of information from Congress; or
- (2) the taking of any personnel action against an employee who lawfully discloses information to Congress.

(e) **DISCLOSURES.** —A disclosure shall not be excluded from this section because—

- (1) the disclosure was made to an individual, including a supervisor, who participated in an activity that the employee reasonably believed to be covered under subsection (b)(1)(B) or the contractor employee reasonably believed to be covered under subsection (c)(1)(A)(ii);
- (2) the disclosure revealed information that had been previously disclosed;
- (3) the disclosure was not made in writing;
- (4) the disclosure was made while the employee was off duty;
- (5) of the amount of time which has passed since the occurrence of the events described in the disclosure; or

(6) the disclosure was made during the normal course of duties of an employee or contractor employee.

(f) **ENFORCEMENT.**—The President shall provide for the enforcement of this section consistent, to the fullest extent possible, with the policies and procedures used to adjudicate alleged violations of section 2302(b)(8) of title 5, United States Code.

(g) **EXISTING RIGHTS PRESERVED.**—Nothing in this section shall be construed to—

(1) preempt or preclude any employee, contractor employee, or applicant for employment, at the Federal Bureau of Investigation from exercising rights provided under any other law, rule, or regulation, including section 2303 of title 5, United States Code; or

(2) repeal section 2303 of title 5, United States Code.

SEMIANNUAL REPORTS ON INVESTIGATIONS OF UNAUTHORIZED DISCLOSURES OF CLASSIFIED INFORMATION

SEC. 1105. [50 U.S.C. § [3235]]

(a) **DEFINITIONS.**—In this section:

(1) **COVERED OFFICIAL.**—The term “covered official” means—

(A) the heads of each element of the intelligence community;
and

(B) the inspectors general with oversight responsibility for an element of the intelligence community.

(2) **INVESTIGATION.**—The term “investigation” means any inquiry, whether formal or informal, into the existence of an unauthorized public disclosure of classified information.

(3) **UNAUTHORIZED DISCLOSURE OF CLASSIFIED INFORMATION.**—The term “unauthorized disclosure of classified information” means any unauthorized disclosure of classified information to any recipient.

(4) **UNAUTHORIZED PUBLIC DISCLOSURE OF CLASSIFIED INFORMATION.**—The term “unauthorized public disclosure of classified information” means the unauthorized disclosure of classified information to a journalist or media organization.

(b) **INTELLIGENCE COMMUNITY REPORTING.**—

(1) **IN GENERAL.**—Not less frequently than once every 6 months, each covered official shall submit to the congressional intelligence committees a report on investigations of unauthorized public disclosures of classified information.

(2) **ELEMENTS.**—Each report submitted under paragraph (1) shall include, with respect to the preceding 6-month period, the following:

(A) The number of investigations opened by the covered official regarding an unauthorized public disclosure of classified information.

(B) The number of investigations completed by the covered official regarding an unauthorized public disclosure of classified information.

(C) Of the number of such completed investigations identified under subparagraph (B), the number referred to the Attorney General for criminal investigation.

(c) DEPARTMENT OF JUSTICE REPORTING.—

(1) IN GENERAL.—Not less frequently than once every 6 months, the Assistant Attorney General for National Security of the Department of Justice, in consultation with the Director of the Federal Bureau of Investigation, shall submit to the congressional intelligence committees, the Committee on the Judiciary of the Senate, and the Committee on the Judiciary of the House of Representatives a report on the status of each referral made to the Department of Justice from any element of the intelligence community regarding an unauthorized disclosure of classified information made during the most recent 365-day period or any referral that has not yet been closed, regardless of the date the referral was made.

(2) CONTENTS.— Each report submitted under paragraph (1) shall include, for each referral covered by the report, at a minimum, the following:

(A) The date the referral was received.

(B) A statement indicating whether the alleged unauthorized disclosure described in the referral was substantiated by the Department of Justice.

(C) A statement indicating the highest level of classification of the information that was revealed in the unauthorized disclosure.

(D) A statement indicating whether an open criminal investigation related to the referral is active.

(E) A statement indicating whether any criminal charges have been filed related to the referral.

(F) A statement indicating whether the Department of Justice has been able to attribute the unauthorized disclosure to a particular entity or individual.

(d) FORM OF REPORTS.—Each report submitted under this section shall be submitted in unclassified form, but may have a classified annex.

NOTICE AND DAMAGE ASSESSMENT WITH RESPECT TO SIGNIFICANT UNAUTHORIZED DISCLOSURE OR COMPROMISE OF CLASSIFIED NATIONAL INTELLIGENCE.

SEC. 1105A.

(a) NOTIFICATION AND DAMAGE ASSESSMENT REQUIREMENTS.—

(1) **REQUIREMENTS.**—If the Director of National Intelligence becomes aware of an actual or potential significant unauthorized disclosure or compromise of classified national intelligence—

(A) as soon as practicable, but not later than 7 days after the date on which the Director becomes so aware, the Director shall notify the congressional intelligence committees of such actual or potential disclosure or compromise; and

(B) in the case of an actual disclosure or compromise, not later than 7 days after the date on which the Director becomes so aware, the Director or the head of any element of the intelligence community from which the significant unauthorized disclosure or compromise originated shall initiate a damage assessment consistent with the procedures set forth in Intelligence Community Directive 732 (relating to the conduct of damage assessments), or successor directive, with respect to such disclosure or compromise.

(2) **CONTENTS OF NOTIFICATION.**—A notification submitted to the congressional intelligence committees under paragraph (1)(A) with respect to an actual or potential significant unauthorized disclosure or compromise of classified national intelligence shall include—

(A) a summary of the facts and circumstances of such disclosure or compromise;

(B) a summary of the contents of the national intelligence revealed or potentially revealed, as the case may be, by such disclosure or compromise;

(C) an initial appraisal of the level of actual or potential damage, as the case may be, to the national security of the United States as a result of such disclosure or compromise; and

(D) in the case of an actual disclosure or compromise, which elements of the intelligence community will be involved in the damage assessment conducted with respect to such disclosure or compromise pursuant to paragraph (1)(B).

(b) DAMAGE ASSESSMENT REPORTING REQUIREMENTS.—

(1) **RECURRING REPORTING REQUIREMENT.**—Not later than 30 days after the date of the initiation of a damage assessment pursuant to subsection (a)(1)(B), and every 90 days thereafter until the completion of the

damage assessment or upon the request of the congressional intelligence committees, the Director of National Intelligence shall—

(A) submit to the congressional intelligence committees copies of any documents or materials disclosed as a result of the significant unauthorized disclosure or compromise of the classified national intelligence that is the subject of the damage assessment; and

(B) provide to the congressional intelligence committees a briefing on such documents and materials and a status of the damage assessment.

(2) FINAL DAMAGE ASSESSMENT.—As soon as practicable after completing a damage assessment pursuant to subsection (a)(1)(B), the Director of National Intelligence shall submit the final damage assessment to the congressional intelligence committees.

(c) NOTIFICATION OF REFERRAL TO DEPARTMENT OF JUSTICE.— If a referral is made to the Department of Justice from any element of the intelligence community regarding a significant unauthorized disclosure or compromise of classified national intelligence under this section, the Director of National Intelligence shall notify the congressional intelligence committees of the referral on the date such referral is made.

INSPECTOR GENERAL EXTERNAL REVIEW PANEL

SEC. 1106. [50 U.S.C. § [3236]]

(a) REQUEST FOR REVIEW.—An individual with a claim described in subsection (b) may submit to the Inspector General of the Intelligence Community a request for a review of such claim by an external review panel convened under subsection (c).

(b) CLAIMS AND INDIVIDUALS DESCRIBED.—A claim described in this subsection is any—

(1) claim by an individual—

(A) that the individual has been subjected to a personnel action that is prohibited under section 1104; and

(B) who has exhausted the applicable review process for the claim pursuant to enforcement of such section; or

(2) claim by an individual—

(A) that he or she has been subjected to a reprisal prohibited by paragraph (1) of section 3001(j) of the Intelligence Reform and Terrorism Prevention Act of 2004 (50 U.S.C. 3341(j)); and

(B) who received a decision on an appeal regarding that claim under paragraph (4) of such section.

(c) EXTERNAL REVIEW PANEL CONVENED.—

(1) DISCRETION TO CONVENE.—Upon receipt of a request under subsection (a) regarding a claim, the Inspector General of the Intelligence Community may, at the discretion of the Inspector General, convene an external review panel under this subsection to review the claim.

(2) MEMBERSHIP.—

(A) COMPOSITION.—An external review panel convened under this subsection shall be composed of three members as follows:

(i) The Inspector General of the Intelligence Community.

(ii) Except as provided in subparagraph (B), two members selected by the Inspector General as the Inspector General considers appropriate on a case-by-case basis from among inspectors general of the following:

(I) The Department of Defense.

(II) The Department of Energy.

(III) The Department of Homeland Security.

(IV) The Department of Justice.

(V) The Department of State.

(VI) The Department of the Treasury.

(VII) The Central Intelligence Agency.

(VIII) The Defense Intelligence Agency.

(IX) The National Geospatial-Intelligence Agency.

(X) The National Reconnaissance Office.

(XI) The National Security Agency.

(B) LIMITATION.—An inspector general of an agency may not be selected to sit on the panel under subparagraph (A)(ii) to review any matter relating to a decision made by such agency.

(C) CHAIRPERSON.—

(i) IN GENERAL.—Except as provided in clause (ii), the chairperson of any panel convened under this subsection shall be the Inspector General of the Intelligence Community.

(ii) CONFLICTS OF INTEREST.—If the Inspector General of the Intelligence Community finds cause to recuse himself or herself from a panel convened under this subsection, the Inspector General of the Intelligence Community shall—

(I) select a chairperson from inspectors general of the elements listed under subparagraph (A)(ii) whom the Inspector General of the Intelligence Community considers appropriate; and
(II) notify the congressional intelligence committees of such selection.

(3) PERIOD OF REVIEW.—Each external review panel convened under this subsection to review a claim shall complete review of the claim no later than 270 days after the date on which the Inspector General convenes the external review panel.

(d) REMEDIES.—

(1) PANEL RECOMMENDATIONS.—If an external review panel convened under subsection (c) determines, pursuant to a review of a claim submitted by an individual under subsection (a), that the individual was the subject of a personnel action prohibited under section 1104 or was subjected to a reprisal prohibited by section 3001(j)(1) of the Intelligence Reform and Terrorism Prevention Act of 2004 (50 U.S.C. 3341(j)(1)), the panel may recommend that the agency head take corrective action—

(A) in the case of an employee or former employee—

(i) to return the employee or former employee, as nearly as practicable and reasonable, to the position such employee or former employee would have held had the reprisal not occurred; or

(ii) reconsider the employee's or former employee's eligibility for access to classified information consistent with national security; or

(B) in any other case, such other action as the external review panel considers appropriate.

(2) AGENCY ACTION.—

(A) IN GENERAL.—Not later than 90 days after the date on which the head of an agency receives a recommendation from an external review panel under paragraph (1), the head shall—

(i) give full consideration to such recommendation; and

(ii) inform the panel and the Director of National Intelligence of what action the head has taken with respect to the recommendation.

(B) FAILURE TO INFORM.—The Director shall notify the President of any failures to comply with subparagraph (A)(ii).

(e) ANNUAL REPORTS.—

(1) IN GENERAL.—Not less frequently than once each year, the Inspector General of the Intelligence Community shall submit to the congressional

intelligence committees and the Director of National Intelligence a report on the activities under this section during the previous year.

(2) CONTENTS.—Subject to such limitations as the Inspector General of the Intelligence Community considers necessary to protect the privacy of an individual who has made a claim described in subsection (b), each report submitted under paragraph (1) shall include, for the period covered by the report, the following:

(A) The determinations and recommendations made by the external review panels convened under this section.

(B) The responses of the heads of agencies that received recommendations from the external review panels.

ANNUAL REPORTS ON INFLUENCE OPERATIONS AND CAMPAIGNS IN THE UNITED STATES BY THE CHINESE COMMUNIST PARTY

SEC. 1107. [50 U.S.C. § 3237]

(a) REQUIREMENT.—On an annual basis, consistent with the protection of intelligence sources and methods, the Director of the National Counterintelligence and Security Center shall submit to the congressional intelligence committees, the Committee on Foreign Affairs of the House of Representatives, and the Committee on Foreign Relations of the Senate a report on the influence operations and campaigns in the United States conducted by the Chinese Communist Party.

(b) CONTENTS.—Each report under subsection (a) shall include the following:

(1) A description of the organization of the United Front Work Department of the People's Republic of China, or the successors of the United Front Work Department, and the links between the United Front Work Department and the Central Committee of the Chinese Communist Party.

(2) An assessment of the degree to which organizations that are associated with or receive funding from the United Front Work Department, particularly such entities operating in the United States, are formally tasked by the Chinese Communist Party or the Government of China.

(3) A description of the efforts by the United Front Work Department and subsidiary organizations of the United Front Work Department to target, coerce, and influence foreign populations, particularly those of ethnic Chinese descent.

(4) An assessment of attempts by the Chinese Embassy, consulates, and organizations affiliated with the Chinese Communist Party (including, at a minimum, the United Front Work Department) to influence the United States-based Chinese Student Scholar Associations.

- (5) A description of the evolution of the role of the United Front Work Department under the leadership of the President of China.
- (6) An assessment of the activities of the United Front Work Department designed to influence the opinions of elected leaders of the United States, or candidates for elections in the United States, with respect to issues of importance to the Chinese Communist Party.
- (7) A listing of all known organizations affiliated with the United Front Work Department that are operating in the United States as of the date of the report.
- (8) An identification of influence activities and operations employed by the Chinese Communist Party against the United States science and technology sectors, specifically employees of the United States Government, researchers, scientists, and students in the science and technology sector in the United States.
- (9) A listing of all known Chinese talent recruitment programs operating in the United States as of the date of the report.
- (10) With respect to reports submitted after the first report, an assessment of the change in goals, tactics, techniques, and procedures of the influence operations and campaigns conducted by the Chinese Communist Party.

(c) COORDINATION.—In carrying out subsection (a), the Director shall coordinate with the Director of the Federal Bureau of Investigation, the Director of the Central Intelligence Agency, the Director of the National Security Agency, and any other relevant head of an element of the intelligence community.

(d) FORM.—Each report submitted under subsection (a) shall be submitted in unclassified form, but may include a classified annex.

[50 U.S.C. § 3237a note] [Congressional Finding]

[Congress finds that the National People’s Republic of China promulgated the Law of the People’s Republic of China on Safeguarding National Security in the Hong Kong Special Administrative Region on June 30, 2020.]

ANNUAL REPORTS ON INFLUENCE OPERATIONS AND CAMPAIGNS IN THE UNITED STATES BY THE RUSSIAN FEDERATION

SEC. 1108. [50 U.S.C. § 3238]

(a) REQUIREMENT.—On an annual basis, the Director of the National Counterintelligence and Security Center shall submit to the congressional intelligence committees a report on the influence operations and campaigns in the United States conducted by the Russian Federation.

(b) CONTENTS.—Each report under subsection (a) shall include the following:

(1) A description and listing of the Russian organizations and persons involved in influence operations and campaigns operating in the United States as of the date of the report.

(2) An assessment of organizations that are associated with or receive funding from organizations and persons identified in paragraph (1), particularly such entities operating in the United States.

(3) A description of the efforts by the organizations and persons identified in paragraph (1) to target, coerce, and influence populations within the United States.

(4) An assessment of the activities or the organizations and persons identified in paragraph (1) designed to influence the opinions of elected leaders of the United States or candidates for election in the United States.

(5) With respect to reports submitted after the first report, an assessment of the change in goals, tactics, techniques, and procedures of the influence operations and campaigns conducted by the organizations and persons identified in paragraph (1).

(c) COORDINATION.—In carrying out subsection (a), the Director shall coordinate with the Director of the Federal Bureau of Investigation, the Director of the Central Intelligence Agency, the Director of the National Security Agency, and any other relevant head of an element of the intelligence community.

(d) FORM.—Each report submitted under subsection (a) shall be submitted in unclassified form, but may include a classified annex.

REQUIREMENT TO BUY CERTAIN SATELLITE COMPONENT FROM AMERICAN SOURCES

SEC. 1109 [50 U.S.C. § 3239]

(a) DEFINITIONS.—In this section:

(1) COVERED ELEMENT OF THE INTELLIGENCE COMMUNITY.—The term ‘covered element of the intelligence community’ means an element of the intelligence community that is not an element of the Department of Defense.

(2) NATIONAL SECURITY SATELLITE.—The term ‘national security satellite’ means a satellite weighing over 400 pounds whose principle purpose is to support the national security or intelligence needs of the United States Government.

(3) UNITED STATES.—The term ‘United States’ means the several States, the District of Columbia, and the territories and possessions of the United States.

(b) REQUIREMENT.—Beginning January 1, 2021, except as provided in subsection (c), a covered element of the intelligence community may not award a

contract for a national security satellite if the satellite uses a star tracker that is not produced in the United States, including with respect to both the software and the hardware of the star tracker.

(c) EXCEPTION.—The head of a covered element of the intelligence community may waive the requirement under subsection (b) if, on a case-by-case basis, the head certifies in writing to the congressional intelligence committees that—

- (1) there is no available star tracker produced in the United States that meets the mission and design requirements of the national security satellite for which the star tracker will be used;
- (2) the cost of a star tracker produced in the United States is unreasonable, based on a market survey; or
- (3) such waiver is necessary for the national security interests of the United States based on an urgent and compelling need

**REPORT ON BEST PRACTICES TO PROTECT PRIVACY, CIVIL LIBERTIES, AND
CIVIL RIGHTS OF CHINESE AMERICANS**

SEC. 1110. [50 U.S.C. 3231]

(a) SENSE OF CONGRESS.—It is the sense of Congress that—

- (1) the People’s Republic of China appears to be specifically targeting the Chinese-American community for intelligence purposes;
- (2) such targeting carries a substantial risk that the loyalty of such Americans may be generally questioned and lead to unacceptable stereotyping, targeting, and racial profiling;
- (3) the United States Government has a duty to warn and protect all Americans including those of Chinese descent from these intelligence efforts by the People’s Republic of China;
- (4) the broad stereotyping, targeting, and racial profiling of Americans of Chinese descent is contrary to the values of the United States and reinforces the flawed narrative perpetuated by the People’s Republic of China that ethnically Chinese individuals worldwide have a duty to support the People’s Republic of China; and
- (5) the United States efforts to combat the People’s Republic of China’s intelligence activities should actively safeguard and promote the constitutional rights of all Chinese Americans.

(b) REPORT.—On an annual basis, the Director of National Intelligence, acting through the Office of Civil Liberties, Privacy, and Transparency, in coordination with the civil liberties and privacy officers of the elements of the intelligence community, shall submit a report to the congressional intelligence committees containing—

- (1) a review of how the policies, procedures, and practices of the intelligence community that govern the intelligence activities and

operations targeting the People’s Republic of China affect policies, procedures, and practices relating to the privacy, civil liberties, and civil rights of Americans of Chinese descent who may be targets of espionage and influence operations by China; and

(2) recommendations to ensure that the privacy, civil liberties, and civil rights of Americans of Chinese descent are sufficiently protected.

(c) FORM.—The report under subsection (b) shall be submitted in unclassified form, but may include a classified annex.

BIENNIAL REPORTS ON FOREIGN BIOLOGICAL THREATS

SEC. 1111 [50 U.S.C. § 3238]

(a) REPORTS. —On a biennial basis until the date that is 10 years after the date of the enactment of the Intelligence Authorization Act for Fiscal Year 2022, the Director of National Intelligence shall submit to the congressional intelligence committees a comprehensive report on the activities, prioritization, and responsibilities of the intelligence community with respect to foreign biological threats emanating from the territory of, or sponsored by, a covered country.

(b) MATTERS INCLUDED. —Each report under subsection (a) shall include, with respect to foreign biological threats emanating from the territory of, or sponsored by, a covered country, the following:

(1) A detailed description of all activities relating to such threats undertaken by each element of the intelligence community, and an assessment of any gaps in such activities.

(2) A detailed description of all duties and responsibilities relating to such threats explicitly authorized or otherwise assigned, exclusively or jointly, to each element of the intelligence community, and an assessment of any identified gaps in such duties or responsibilities.

(3) A description of the coordination among the relevant elements of the intelligence community with respect to the activities specified in paragraph (1) and the duties and responsibilities specified in paragraph (2).

(2).

(4) An inventory of the strategies, plans, policies, and interagency agreements of the intelligence community relating to the collection, monitoring, analysis, mitigation, and attribution of such threats, and an assessment of any identified gaps therein.

(5) A description of the coordination and interactions among the relevant elements of the intelligence community and non-intelligence community partners.

(6) An assessment of foreign malign influence efforts relating to such threats, including any foreign academics engaged in such efforts, and a description of how the intelligence community contributes to efforts by

non-intelligence community partners to counter such foreign malign influence.

(c) FORM. —Each report submitted under subsection (a) may be submitted in classified form, but if so submitted shall include an unclassified executive summary.

(d) DEFINITIONS. —In this section:

(1) COVERED COUNTRY. —The term “covered country” means—

(A) China;

(B) Iran;

(C) North Korea;

(D) Russia; and

(E) any other foreign country—

(i) from which the Director of National Intelligence determines a biological threat emanates; or

(ii) that the Director determines has a known history of, or has been assessed as having conditions present for, infectious disease outbreaks or epidemics.

(2) FOREIGN BIOLOGICAL THREAT. —The term “foreign biological threat” means biological warfare, bioterrorism, naturally occurring infectious diseases, or accidental exposures to biological materials, without regard to whether the threat originates from a state actor, a non-state actor, natural conditions, or an undetermined source.

(3) FOREIGN MALIGN INFLUENCE. —The term “foreign malign influence” has the meaning given such term in section 119C(e) of this Act.

(4) NON-INTELLIGENCE COMMUNITY PARTNER. —The term “non-intelligence community partner” means a Federal department or agency that is not an element of the intelligence community.

**ANNUAL REPORTS ON CERTAIN CYBER VULNERABILITIES
PROCURED BY INTELLIGENCE COMMUNITY AND FOREIGN
COMMERCIAL PROVIDERS OF CYBER VULNERABILITIES**

SEC.1112 [50 U.S.C. § 3141]

(a) ANNUAL REPORTS. —On an annual basis through 2026, the Director of the Central Intelligence Agency and the Director of the National Security Agency, in coordination with the Director of National Intelligence, shall jointly submit to the congressional intelligence committees a report containing information on foreign commercial providers and the cyber vulnerabilities procured by the intelligence community through foreign commercial providers.

(b) ELEMENTS. —Each report under subsection (a) shall include, with respect to the period covered by the report, the following:

(1) A description of each cyber vulnerability procured through a foreign commercial provider, including—

- (A) a description of the vulnerability;
- (B) the date of the procurement;
- (C) whether the procurement consisted of only that vulnerability or included other vulnerabilities;
- (D) the cost of the procurement;
- (E) the identity of the commercial provider and, if the commercial provider was not the original supplier of the vulnerability, a description of the original supplier; and
- (F) the country of origin of the vulnerability; and
- (G) an assessment of the ability of the intelligence community to use the vulnerability, including whether such use will be operational or for research and development, and the approximate timeline for such use.

(2) An assessment of foreign commercial providers that—

- (A) pose a significant threat to the national security of the United States; or
- (B) have provided cyber vulnerabilities to any foreign government that—
 - (i) has used the cyber vulnerabilities to target United States persons, the United States Government, journalists, or dissidents; or
 - (ii) has an established pattern or practice of violating human rights or suppressing dissent.

(3) An assessment of whether the intelligence community has conducted business with the foreign commercial providers identified under paragraph (2) during the 5-year period preceding the date of the report.

(c) FORM.—Each report under subsection (a) may be submitted in classified form.

(d) DEFINITIONS.—In this section:

(1) COMMERCIAL PROVIDER.—The term “commercial provider” means any person that sells, or acts as a broker, for a cyber vulnerability.

(2) CYBER VULNERABILITY.—The term “cyber vulnerability” means any tool, exploit, vulnerability, or code that is intended to compromise a device, network, or system, including such a tool, exploit, vulnerability, or code procured by the intelligence community for purposes of research and development.

**PERIODIC REPORTS ON TECHNOLOGY STRATEGY OF INTELLIGENCE
COMMUNITY**

SEC. 1113. [50 U.S.C. 3243]

(a) **REPORTS.**—On a basis that is not less frequent than once every 4 years, the Director of National Intelligence, in coordination with the Director of the Office of Science and Technology Policy, the Secretary of Commerce, and the heads of such other agencies as the Director considers appropriate, shall submit to the congressional intelligence committees a comprehensive report on the technology strategy of the intelligence community, which shall be designed to support the maintenance of the leadership of the United States.

(b) **ELEMENTS.**—Each report submitted under subsection (a) shall include the following:

- (1) An assessment of technologies critical to the national security of the United States, particularly those technologies with respect to which foreign countries that are adversarial to the United States have or are poised to match or surpass the technology leadership of the United States.
- (2) A review of current technology policies of the intelligence community, including long-term goals.
- (3) An identification of sectors and supply chains the Director determines to be of the greatest strategic importance to national security.
- (4) An identification of opportunities to protect the leadership of the United States, and the allies and partners of the United States, in critical technologies, including through targeted export controls, investment screening, and counterintelligence activities.
- (5) An identification of research and development areas the Director determines critical to the national security of the United States, including areas in which the private sector does not focus.
- (6) Recommendations for growing talent in key critical and emerging technologies and enhancing the ability of the intelligence community to recruit and retain individuals with critical skills relating to such technologies.
- (7) An identification of opportunities to improve the leadership of the United States in critical technologies, including opportunities to develop international partnerships to reinforce domestic policy actions, develop new markets, engage in collaborative research, and maintain an international environment that reflects the values of the United States and protects the interests of the United States.
- (8) A technology annex to establish an approach for the identification, prioritization, development, and fielding of emerging technologies critical to the mission of the intelligence community.

(9) Such other information as the Director determines may be necessary to inform Congress on matters relating to the technology strategy of the intelligence community and related implications for the national security of the United States.

(c) FORM OF ANNEX.—Each annex submitted under subsection (b)(8) may be submitted in classified form.

ANNUAL REPORT ON REPORTING REQUIREMENTS

SEC. 1114.

(a) ANNUAL REPORT REQUIRED.—Not later than March 1 of each fiscal year, the Director of National Intelligence shall submit to the congressional intelligence committees, the Committee on Appropriations of the Senate, and the Committee on Appropriations of the House of Representatives a report detailing all congressionally mandated reporting requirements applicable to Office of the Director of National Intelligence for the upcoming fiscal year.

(b) CONTENTS.—Each report submitted pursuant to subsection (a) shall include, for the fiscal year covered by the report and for each congressionally mandated reporting requirement detailed in the report:

- (1) A description of the reporting requirement.
- (2) A citation to the provision of law (or other source of congressional directive) imposing the reporting requirement.
- (3) Whether the reporting requirement is recurring, conditional, or subject to a termination provision.
- (4) Whether the Director recommends repealing or modifying the requirement.

(c) FORM.—Each report submitted pursuant to subsection (a) may be submitted in classified form.

**INTELLIGENCE REFORM AND TERRORISM
PREVENTION ACT OF 2004^[1]**

[Public Law 108-458; 118 STAT. 3638; December 17, 2004]

AN ACT To reform the intelligence community and the intelligence and intelligence-related activities of the United States Government, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the “Intelligence Reform and Terrorism Prevention Act of 2004”.

(b) TABLE OF CONTENTS.—The table of contents for this Act is as follows:

TITLE I—REFORM OF THE INTELLIGENCE COMMUNITY

SUBTITLE A—ESTABLISHMENT OF DIRECTOR OF NATIONAL INTELLIGENCE

Sec. 1016. Information sharing.

SUBTITLE F—PRIVACY AND CIVIL LIBERTIES

Sec. 1061. Privacy and Civil Liberties Oversight Board.

Sec. 1062. Privacy and civil liberties officers.

TITLE III—SECURITY CLEARANCES

Sec. 3001. Security clearances.

TITLE I—REFORM OF THE INTELLIGENCE COMMUNITY

**SUBTITLE A—ESTABLISHMENT OF THE DIRECTOR OF NATIONAL
INTELLIGENCE**

¹ Only select provisions are included, as reflected in the table of contents excerpt.

INFORMATION SHARING

SEC. 1016. [6 U.S.C. § 485]

(a) DEFINITIONS—In this section:

- (1) **HOMELAND SECURITY INFORMATION.**—The term “homeland security information” has the meaning given that term in section 892(f) of the Homeland Security Act of 2002 (6 U.S.C. 482(f)).
- (2) **INFORMATION SHARING COUNCIL.**—The term “Information Sharing Council” means the Information Systems Council established by Executive Order 13356, or any successor body designated by the President, and referred to under subsection (g).
- (3) **INFORMATION SHARING ENVIRONMENT.**—The terms “information sharing environment” and “ISE” mean an approach that facilitates the sharing of terrorism and homeland security information, which may include any method determined necessary and appropriate for carrying out this section.
- (4) **PROGRAM MANAGER.**—The term “program manager” means the program manager designated under subsection (f).
- (5) **TERRORISM INFORMATION.**—The term “terrorism information”—
 - (A) means all information, whether collected, produced, or distributed by intelligence, law enforcement, military, homeland security, or other activities relating to—
 - (i) the existence, organization, capabilities, plans, intentions, vulnerabilities, means of finance or material support, or activities of foreign or international terrorist groups or individuals, or of domestic groups or individuals involved in transnational terrorism;
 - (ii) threats posed by such groups or individuals to the United States, United States persons, or United States interests, or to those of other nations;
 - (iii) communications of or by such groups or individuals;or
 - (iv) groups or individuals reasonably believed to be assisting or associated with such groups or individuals;and
 - (B) includes weapons of mass destruction information.
- (6) **WEAPONS OF MASS DESTRUCTION INFORMATION.**—The term “weapons of mass destruction information” means information that could reasonably be expected to assist in the development, proliferation, or use of a weapon of mass destruction (including a chemical, biological, radiological, or nuclear weapon) that could be used by a terrorist or a terrorist organization against the United States, including information

about the location of any stockpile of nuclear materials that could be exploited for use in such a weapon that could be used by a terrorist or a terrorist organization against the United States.

(b) INFORMATION SHARING ENVIRONMENT.—

(1) ESTABLISHMENT.—The President shall—

(A) create an information sharing environment for the sharing of terrorism information in a manner consistent with national security and with applicable legal standards relating to privacy and civil liberties;

(B) designate the organizational and management structures that will be used to operate and manage the ISE; and

(C) determine and enforce the policies, directives, and rules that will govern the content and usage of the ISE.

(2) ATTRIBUTES.—The President shall, through the structures described in subparagraphs (B) and (C) of paragraph (1), ensure that the ISE provides and facilitates the means for sharing terrorism information among all appropriate Federal, State, local, and tribal entities, and the private sector through the use of policy guidelines and technologies. The President shall, to the greatest extent practicable, ensure that the ISE provides the functional equivalent of, or otherwise supports, a decentralized, distributed, and coordinated environment that—

(A) connects existing systems, where appropriate, provides no single points of failure, and allows users to share information among agencies, between levels of government, and, as appropriate, with the private sector;

(B) ensures direct and continuous online electronic access to information;

(C) facilitates the availability of information in a form and manner that facilitates its use in analysis, investigations and operations;

(D) builds upon existing systems capabilities currently in use across the Government;

(E) employs an information access management approach that controls access to data rather than just systems and networks, without sacrificing security;

(F) facilitates the sharing of information at and across all levels of security;

(G) provides directory services, or the functional equivalent, for locating people and information;

(H) incorporates protections for individuals' privacy and civil liberties;

- (I) incorporates strong mechanisms to enhance accountability and facilitate oversight, including audits, authentication, and access controls;
- (J) integrates the information within the scope of the information sharing environment, including any such information in legacy technologies;
- (K) integrates technologies, including all legacy technologies, through Internet-based services, consistent with appropriate security protocols and safeguards, to enable connectivity among required users at the Federal, State, and local levels;
- (L) allows the full range of analytic and operational activities without the need to centralize information within the scope of the information sharing environment;
- (M) permits analysts to collaborate both independently and in a group (commonly known as “collective and noncollective collaboration”), and across multiple levels of national security information and controlled unclassified information;
- (N) provides a resolution process that enables changes by authorized officials regarding rules and policies for the access, use, and retention of information within the scope of the information sharing environment; and
- (O) incorporates continuous, real-time, and immutable audit capabilities, to the maximum extent practicable.

(3) DELEGATION.—

(A) IN GENERAL.—Subject to subparagraph (B), the President may delegate responsibility for carrying out this subsection.

(B) LIMITATION.—The President may not delegate responsibility for carrying out this subsection to the Director of National Intelligence.

(c) PRELIMINARY REPORT.—Not later than 180 days after the date of the enactment of this Act, the program manager shall, in consultation with the Information Sharing Council—

- (1) submit to the President and Congress a description of the technological, legal, and policy issues presented by the creation of the ISE, and the way in which these issues will be addressed;
- (2) establish an initial capability to provide electronic directory services, or the functional equivalent, to assist in locating in the Federal Government intelligence and terrorism information and people with relevant knowledge about intelligence and terrorism information; and
- (3) conduct a review of relevant current Federal agency capabilities, databases, and systems for sharing information.

(d) **GUIDELINES AND REQUIREMENTS.**—As soon as possible, but in no event later than 270 days after the date of the enactment of this Act, the President shall—

(1) leverage all ongoing efforts consistent with establishing the ISE and issue guidelines for acquiring, accessing, sharing, and using information, including guidelines to ensure that information is provided in its most shareable form, such as by using tearlines to separate out data from the sources and methods by which the data are obtained;

(2) in consultation with the Privacy and Civil Liberties Oversight Board established under section 1061, issue guidelines that—

(A) protect privacy and civil liberties in the development and use of the ISE; and

(B) shall be made public, unless nondisclosure is clearly necessary to protect national security; and

(3) require the heads of Federal departments and agencies to promote a culture of information sharing by—

(A) reducing disincentives to information sharing, including over-classification of information and unnecessary requirements for originator approval, consistent with applicable laws and regulations; and

(B) providing affirmative incentives for information sharing.

(e) **IMPLEMENTATION PLAN REPORT.**—Not later than one year after the date of the enactment of this Act, the President shall, with the assistance of the program manager, submit to Congress a report containing an implementation plan for the ISE. The report shall include the following:

(1) A description of the functions, capabilities, resources, and conceptual design of the ISE, including standards.

(2) A description of the impact on enterprise architectures of participating agencies.

(3) A budget estimate that identifies the incremental costs associated with designing, testing, integrating, deploying, and operating the ISE.

(4) A project plan for designing, testing, integrating, deploying, and operating the ISE.

(5) The policies and directives referred to in subsection (b)(1)(C), as well as the metrics and enforcement mechanisms that will be utilized.

(6) Objective, systemwide performance measures to enable the assessment of progress toward achieving the full implementation of the ISE.

(7) A description of the training requirements needed to ensure that the ISE will be adequately implemented and properly utilized.

(8) A description of the means by which privacy and civil liberties will be protected in the design and operation of the ISE.

(9) The recommendations of the program manager, in consultation with the Information Sharing Council, regarding whether, and under what conditions, the ISE should be expanded to include other intelligence information.

(10) A delineation of the roles of the Federal departments and agencies that will participate in the ISE, including an identification of the agencies that will deliver the infrastructure needed to operate and manage the ISE (as distinct from individual department or agency components that are part of the ISE), with such delineation of roles to be consistent with—

(A) the authority of the Director of National Intelligence under this title, and the amendments made by this title, to set standards for information sharing throughout the intelligence community; and

(B) the authority of the Secretary of Homeland Security and the Attorney General, and the role of the Department of Homeland Security and the Department of Justice, in coordinating with State, local, and tribal officials and the private sector.

(11) The recommendations of the program manager, in consultation with the Information Sharing Council, for a future management structure for the ISE, including whether the position of program manager should continue to remain in existence.

(f) PROGRAM MANAGER.—

(1) DESIGNATION.—Not later than 120 days after the date of the enactment of this Act, with notification to Congress, the President shall designate an individual as the program manager responsible for information sharing across the Federal Government. Beginning on the date of the enactment of the Damon Paul Nelson and Matthew Young Pollard Intelligence Authorization Act for Fiscal Years 2018, 2019 and 2020, each individual designated as the program manager shall be appointed by the Director of National Intelligence. The program manager, in consultation with the head of any affected department or agency, shall have and exercise government-wide authority over the sharing of information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information, by all Federal departments, agencies, and components, irrespective of the Federal department, agency, or component in which the program manager may be administratively located, except as otherwise expressly provided by law.

(2) DUTIES AND RESPONSIBILITIES.—

(A) IN GENERAL.—The program manager shall, in consultation with the Information Sharing Council—

- (i) plan for and oversee the implementation of, and manage, the ISE;
- (ii) assist in the development of policies, as appropriate, to foster the development and proper operation of the ISE;
- (iii) consistent with the direction and policies issued by the President, the Director of National Intelligence, and the Director of the Office of Management and Budget, issue governmentwide procedures, guidelines, instructions, and functional standards, as appropriate, for the management, development, and proper operation of the ISE;
- (iv) identify and resolve information sharing disputes between Federal departments, agencies, and components; and
- (v) assist, monitor, and assess the implementation of the ISE by Federal departments and agencies to ensure adequate progress, technological consistency and policy compliance; and regularly report the findings to Congress.

(B) CONTENT OF POLICIES, PROCEDURES, GUIDELINES, RULES, AND STANDARDS.—The policies, procedures, guidelines, rules, and standards under subparagraph (A)(ii) shall—

- (i) take into account the varying missions and security requirements of agencies participating in the ISE;
- (ii) address development, implementation, and oversight of technical standards and requirements;
- (iii) take into account ongoing and planned efforts that support development, implementation and management of the ISE;
- (iv) address and facilitate information sharing between and among departments and agencies of the intelligence community, the Department of Defense, the homeland security community and the law enforcement community;
- (v) address and facilitate information sharing between Federal departments and agencies and State, tribal, and local governments;
- (vi) address and facilitate, as appropriate, information sharing between Federal departments and agencies and the private sector;

- (vii) address and facilitate, as appropriate, information sharing between Federal departments and agencies with foreign partners and allies; and
- (viii) ensure the protection of privacy and civil liberties.

(g) INFORMATION SHARING COUNCIL.—

(1) ESTABLISHMENT.—There is established an Information Sharing Council that shall assist the President and the program manager in their duties under this section. The Information Sharing Council shall serve until removed from service or replaced by the President (at the sole discretion of the President) with a successor body.

(2) SPECIFIC DUTIES.—In assisting the President and the program manager in their duties under this section, the Information Sharing Council shall—

(A) advise the President and the program manager in developing policies, procedures, guidelines, roles, and standards necessary to establish, implement, and maintain the ISE;

(B) work to ensure coordination among the Federal departments and agencies participating in the ISE in the establishment, implementation, and maintenance of the ISE;

(C) identify and, as appropriate, recommend the consolidation and elimination of current programs, systems, and processes used by Federal departments and agencies to share information, and recommend, as appropriate, the redirection of existing resources to support the ISE;

(D) identify gaps, if any, between existing technologies, programs and systems used by Federal departments and agencies to share information and the parameters of the proposed information sharing environment;

(E) recommend solutions to address any gaps identified under subparagraph (D);

(F) recommend means by which the ISE can be extended to allow interchange of information between Federal departments and agencies and appropriate authorities of State and local governments;

(G) assist the program manager in identifying and resolving information sharing disputes between Federal departments, agencies, and components;

(H) identify appropriate personnel for assignment to the program manager to support staffing needs identified by the program manager; and

(I) recommend whether or not, and by which means, the ISE should be expanded so as to allow future expansion encompassing other relevant categories of information.

(3) CONSULTATION.—In performing its duties, the Information Sharing Council shall consider input from persons and entities outside the Federal Government having significant experience and expertise in policy, technical matters, and operational matters relating to the ISE.

(4) INAPPLICABILITY OF CHAPTER 10 OF TITLE 5, UNITED STATES CODE.—The Information Sharing Council (including any subsidiary group of the Information Sharing Council) shall not be subject to the requirements of chapter 10 of title 5, United States Code.

(5) DETAILEES.—Upon a request by the Director of National Intelligence, the departments and agencies represented on the Information Sharing Council shall detail to the program manager, on a reimbursable basis, appropriate personnel identified under paragraph (2)(H).

(h) AGENCY RESPONSIBILITIES.—The head of each department or agency that possesses or uses intelligence or terrorism information, operates a system in the ISE, or otherwise participates (or expects to participate) in the ISE shall—

(1) ensure full department or agency compliance with information sharing policies, procedures, guidelines, rules, and standards established under subsections (b) and (f);

(2) ensure the provision of adequate resources for systems and activities supporting operation of and participation in the ISE;

(3) ensure full department or agency cooperation in the development of the ISE to implement governmentwide information sharing; and

(4) submit, at the request of the President or the program manager, any reports on the implementation of the requirements of the ISE within such department or agency.

(i) REPORT ON THE INFORMATION SHARING ENVIRONMENT.—

(1) IN GENERAL.—Not later than 180 days after the date of enactment of the Implementing Recommendations of the 9/11 Commission Act of 2007, the President shall report to the Committee on Homeland Security and Governmental Affairs of the Senate, the Select Committee on Intelligence of the Senate, the Committee on Homeland Security of the House of Representatives, and the Permanent Select Committee on Intelligence of the House of Representatives on the feasibility of—

(A) eliminating the use of any marking or process (including “Originator Control”) intended to, or having the effect of, restricting the sharing of information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass

destruction information, between and among participants in the information sharing environment, unless the President has—

(i) specifically exempted categories of information from such elimination; and

(ii) reported that exemption to the committees of Congress described in the matter preceding this subparagraph; and

(B) continuing to use Federal agency standards in effect on such date of enactment for the collection, sharing, and access to information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information, relating to citizens and lawful permanent residents;

(C) replacing the standards described in subparagraph (B) with a standard that would allow mission-based or threat-based permission to access or share information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information, for a particular purpose that the Federal Government, through an appropriate process established in consultation with the Privacy and Civil Liberties Oversight Board established under section 1061, has determined to be lawfully permissible for a particular agency, component, or employee (commonly known as an “authorized use” standard); and

(D) the use of anonymized data by Federal departments, agencies, or components collecting, possessing, disseminating, or handling information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information, in any cases in which—

(i) the use of such information is reasonably expected to produce results materially equivalent to the use of information that is transferred or stored in a non-anonymized form; and

(ii) such use is consistent with any mission of that department, agency, or component (including any mission under a Federal statute or directive of the President) that involves the storage, retention, sharing, or exchange of personally identifiable information.

(2) DEFINITION.—In this subsection, the term “anonymized data” means data in which the individual to whom the data pertains is not identifiable

with reasonable efforts, including information that has been encrypted or hidden through the use of other technology.

(j) **ADDITIONAL POSITIONS.**—The program manager is authorized to hire not more than 40 full-time employees to assist the program manager in—

(1) activities associated with the implementation of the information sharing environment, including—

(A) implementing the requirements under subsection (b)(2); and

(B) any additional implementation initiatives to enhance and expedite the creation of the information sharing environment; and

(2) identifying and resolving information sharing disputes between Federal departments, agencies, and components under subsection (f)(2)(A)(iv).

(k) **AUTHORIZATION OF APPROPRIATIONS.**—There is authorized to be appropriated to carry out this section \$30,000,000 for each of fiscal years 2008 and 2009.

SUBTITLE F—PRIVACY AND CIVIL LIBERTIES

PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD

SEC. 1061. [42 U.S.C. § 2000ee]

(a) **IN GENERAL.**—There is established as an independent agency within the executive branch a Privacy and Civil Liberties Oversight Board (referred to in this section as the “Board”).

(b) **FINDINGS.**—Consistent with the report of the National Commission on Terrorist Attacks Upon the United States, Congress makes the following findings:

(1) In conducting the war on terrorism, the Government may need additional powers and may need to enhance the use of its existing powers.

(2) This shift of power and authority to the Government calls for an enhanced system of checks and balances to protect the precious liberties that are vital to our way of life and to ensure that the Government uses its powers for the purposes for which the powers were given.

(3) The National Commission on Terrorist Attacks Upon the United States correctly concluded that “The choice between security and liberty is a false choice, as nothing is more likely to endanger America’s liberties than the success of a terrorist attack at home. Our history has shown us that insecurity threatens liberty. Yet, if our liberties are curtailed, we lose the values that we are struggling to defend.”

(c) PURPOSE.—The Board shall—

- (1) analyze and review actions the executive branch takes to protect the Nation from terrorism, ensuring that the need for such actions is balanced with the need to protect privacy and civil liberties; and
- (2) ensure that liberty concerns are appropriately considered in the development and implementation of laws, regulations, and policies related to efforts to protect the Nation against terrorism.

(d) FUNCTIONS.—

(1) ADVICE AND COUNSEL ON POLICY DEVELOPMENT AND IMPLEMENTATION.—The Board shall—

- (A) review proposed legislation, regulations, and policies related to efforts to protect the Nation from terrorism, including the development and adoption of information sharing guidelines under subsections (d) and (f) of section 1016;
- (B) review the implementation of new and existing legislation, regulations, and policies related to efforts to protect the Nation from terrorism, including the implementation of information sharing guidelines under subsections (d) and (f) of section 1016;
- (C) advise the President and the departments, agencies, and elements of the executive branch to ensure that privacy and civil liberties are appropriately considered in the development and implementation of such legislation, regulations, policies, and guidelines; and
- (D) in providing advice on proposals to retain or enhance a particular governmental power, consider whether the department, agency, or element of the executive branch has established—
 - (i) that the need for the power is balanced with the need to protect privacy and civil liberties;
 - (ii) that there is adequate supervision of the use by the executive branch of the power to ensure protection of privacy and civil liberties; and
 - (iii) that there are adequate guidelines and oversight to properly confine its use.

(2) OVERSIGHT.—The Board shall continually review—

- (A) the regulations, policies, and procedures, and the implementation of the regulations, policies, and procedures, of the departments, agencies, and elements of the executive branch relating to efforts to protect the Nation from terrorism to ensure that privacy and civil liberties are protected;
- (B) the information sharing practices of the departments, agencies, and elements of the executive branch relating to efforts to protect the Nation from terrorism to determine whether they

appropriately protect privacy and civil liberties and adhere to the information sharing guidelines issued or developed under subsections (d) and (f) of section 1016 and to other governing laws, regulations, and policies regarding privacy and civil liberties; and

(C) other actions by the executive branch relating to efforts to protect the Nation from terrorism to determine whether such actions—

- (i) appropriately protect privacy and civil liberties; and
- (ii) are consistent with governing laws, regulations, and policies regarding privacy and civil liberties.

(3) RELATIONSHIP WITH PRIVACY AND CIVIL LIBERTIES OFFICERS.—
The Board shall—

- (A) receive and review reports and other information from privacy officers and civil liberties officers under section 1062;
- (B) when appropriate, make recommendations to such privacy officers and civil liberties officers regarding their activities; and
- (C) when appropriate, coordinate the activities of such privacy officers and civil liberties officers on relevant interagency matters.

(4) TESTIMONY.—The members of the Board shall appear and testify before Congress upon request.

(e) REPORTS.—

(1) IN GENERAL.—The Board shall—

- (A) receive and review reports from privacy officers and civil liberties officers under section 1062; and
- (B) periodically submit, not less than semiannually, reports—
 - (i)(I) to the appropriate committees of Congress, including the Committee on the Judiciary of the Senate, the Committee on the Judiciary of the House of Representatives, the Committee on Homeland Security and Governmental Affairs of the Senate, the Committee on Homeland Security of the House of Representatives, the Committee on Oversight and Government Reform of the House of Representatives, the Select Committee on Intelligence of the Senate, and the Permanent Select Committee on Intelligence of the House of Representatives; and
 - (II) to the President; and
 - (ii) which shall be in unclassified form to the greatest extent possible, with a classified annex where necessary.

(2) CONTENTS.—Not less than 2 reports submitted each year under paragraph (1)(B) shall include—

- (A) a description of the major activities of the Board during the preceding period;
- (B) information on the findings, conclusions, and recommendations of the Board resulting from its advice and oversight functions under subsection (d);
- (C) the minority views on any findings, conclusions, and recommendations of the Board resulting from its advice and oversight functions under subsection (d);
- (D) each proposal reviewed by the Board under subsection (d)(1) that—
 - (i) the Board advised against implementation; and
 - (ii) notwithstanding such advice, actions were taken to implement; and
- (E) for the preceding period, any requests submitted under subsection (g)(1)(D) for the issuance of subpoenas that were modified or denied by the Attorney General.

(f) INFORMING THE PUBLIC.—The Board—

- (1) shall make its reports, including its reports to Congress, available to the public to the greatest extent that is consistent with the protection of classified information and applicable law; and
- (2) shall hold public hearings and otherwise inform the public of its activities, as appropriate and in a manner consistent with the protection of classified information and applicable law, but may, notwithstanding section 552b of title 5, United States Code, meet or otherwise communicate in any number to confer or deliberate in a manner that is closed to the public.

(g) ACCESS TO INFORMATION.—

(1) AUTHORIZATION.—If determined by the Board to be necessary to carry out its responsibilities under this section, the Board is authorized to—

- (A) have access from any department, agency, or element of the executive branch, or any Federal officer or employee of any such department, agency, or element, to all relevant records, reports, audits, reviews, documents, papers, recommendations, or other relevant material, including classified information consistent with applicable law;
- (B) interview, take statements from, or take public testimony from personnel of any department, agency, or element of the executive branch, or any Federal officer or employee of any such department, agency, or element;

(C) request information or assistance from any State, tribal, or local government; and

(D) at the direction of a majority of the members of the Board, submit a written request to the Attorney General of the United States that the Attorney General require, by subpoena, persons (other than departments, agencies, and elements of the executive branch) to produce any relevant information, documents, reports, answers, records, accounts, papers, and other documentary or testimonial evidence.

(2) REVIEW OF SUBPOENA REQUEST.—

(A) IN GENERAL.—Not later than 30 days after the date of receipt of a request by the Board under paragraph (1)(D), the Attorney General shall—

(i) issue the subpoena as requested; or

(ii) provide the Board, in writing, with an explanation of the grounds on which the subpoena request has been modified or denied.

(B) NOTIFICATION.—If a subpoena request is modified or denied under subparagraph (A)(ii), the Attorney General shall, not later than 30 days after the date of that modification or denial, notify the Committee on the Judiciary of the Senate and the Committee on the Judiciary of the House of Representatives.

(3) ENFORCEMENT OF SUBPOENA.—In the case of contumacy or failure to obey a subpoena issued pursuant to paragraph (1)(D), the United States district court for the judicial district in which the subpoenaed person resides, is served, or may be found may issue an order requiring such person to produce the evidence required by such subpoena.

(4) AGENCY COOPERATION.—Whenever information or assistance requested under subparagraph (A) or (B) of paragraph (1) is, in the judgment of the Board, unreasonably refused or not provided, the Board shall report the circumstances to the head of the department, agency, or element concerned without delay. The head of the department, agency, or element concerned shall ensure that the Board is given access to the information, assistance, material, or personnel the Board determines to be necessary to carry out its functions.

(5) ACCESS.—Nothing in this section shall be construed to authorize the Board, or any agent thereof, to gain access to information regarding an activity covered by section 503(a) of the National Security Act of 1947 (50 U.S.C. 3093(a)).

(h) MEMBERSHIP.—

(1) MEMBERS.—The Board shall be composed of a full-time chairman and 4 additional members, who shall be appointed by the President, by and with the advice and consent of the Senate.

(2) QUALIFICATIONS.—Members of the Board shall be selected solely on the basis of their professional qualifications, achievements, public stature, expertise in civil liberties and privacy, and relevant experience, and without regard to political affiliation, but in no event shall more than 3 members of the Board be members of the same political party. The President shall, before appointing an individual who is not a member of the same political party as the President, consult with the leadership of that party, if any, in the Senate and House of Representatives.

(3) INCOMPATIBLE OFFICE.—An individual appointed to the Board may not, while serving on the Board, be an elected official, officer, or employee of the Federal Government, other than in the capacity as a member of the Board.

(4) TERM.—

(A) COMMENCEMENT.—Each member of the Board shall serve a term of 6 years, commencing on the date of the appointment of the member to the Board.

(B) REAPPOINTMENT.—A member may be reappointed to one or more additional terms.

(C) VACANCY.—A vacancy on the Board shall be filled in the manner in which the original appointment was made.

(D) Extension.—upon the expiration of the term of office of a member, the member may continue to serve for up to one year after the date of expiration, at the election of the member—

(i) during the period preceding the reappointment of the member pursuant to subparagraph (b); or

(ii) until the member's successor has been appointed and qualified.

(5) QUORUM AND MEETINGS.—The Board shall meet upon the call of the chairman or a majority of its members. Three members of the Board shall constitute a quorum.

(i) COMPENSATION AND TRAVEL EXPENSES.—

(1) COMPENSATION.—

(A) CHAIRMAN.—The chairman of the Board shall be compensated at the rate of pay payable for a position at level III of the Executive Schedule under section 5314 of title 5, United States Code.

(B) MEMBERS.—Each member of the Board shall be compensated at a rate of pay payable for a position at level IV of

the Executive Schedule under section 5315 of title 5, United States Code, for each day during which that member is engaged in the actual performance of the duties of the Board.

(2) TRAVEL EXPENSES.—Members of the Board shall be allowed travel expenses, including per diem in lieu of subsistence, at rates authorized for persons employed intermittently by the Government under section 5703(b) of title 5, United States Code, while away from their homes or regular places of business in the performance of services for the Board.

(j) STAFF.—

(1) APPOINTMENT AND COMPENSATION.—The chairman of the Board, in accordance with rules agreed upon by the Board, shall appoint and fix the compensation of a full-time executive director and such other personnel as may be necessary to enable the Board to carry out its functions, without regard to the provisions of title 5, United States Code, governing appointments in the competitive service, and without regard to the provisions of chapter 51 and subchapter III of chapter 53 of such title relating to classification and General Schedule pay rates, except that no rate of pay fixed under this subsection may exceed the equivalent of that payable for a position at level V of the Executive Schedule under section 5316 of title 5, United States Code.

(2) APPOINTMENT IN ABSENCE OF CHAIRMAN.—If the position of chairman of the Board is vacant, during the period of the vacancy, the Board, at the direction of the unanimous vote of the serving members of the Board, may exercise the authority of the chairman under paragraph (1).

(3) DETAILEES.—Any Federal employee may be detailed to the Board without reimbursement from the Board, and such detailee shall retain the rights, status, and privileges of the detailee's regular employment without interruption.

(4) CONSULTANT SERVICES.—The Board may procure the temporary or intermittent services of experts and consultants in accordance with section 3109 of title 5, United States Code, at rates that do not exceed the daily rate paid a person occupying a position at level IV of the Executive Schedule under section 5315 of such title.

(k) SECURITY CLEARANCES.—

(1) IN GENERAL.—The appropriate departments, agencies, and elements of the executive branch shall cooperate with the Board to expeditiously provide the Board members and staff with appropriate security clearances to the extent possible under existing procedures and requirements.

(2) RULES AND PROCEDURES.—After consultation with the Secretary of Defense, the Attorney General, and the Director of National Intelligence,

the Board shall adopt rules and procedures of the Board for physical, communications, computer, document, personnel, and other security relating to carrying out the functions of the Board.

- (l) **TREATMENT AS AGENCY, NOT AS ADVISORY COMMITTEE.**—The Board—
- (1) is an agency (as defined in section 551(1) of title 5, United States Code); and
 - (2) is not an advisory committee (as defined in section 3(2) of the Federal Advisory Committee Act (5 U.S.C. App.)).
- (m) **AUTHORIZATION OF APPROPRIATIONS.**—There are authorized to be appropriated to carry out this section amounts as follows:
- (1) For fiscal year 2008, \$5,000,000.
 - (2) For fiscal year 2009, \$6,650,000.
 - (3) For fiscal year 2010, \$8,300,000.
 - (4) For fiscal year 2011, \$10,000,000.
 - (5) For fiscal year 2012 and each subsequent fiscal year, such sums as may be necessary.

PRIVACY AND CIVIL LIBERTIES OFFICERS

SEC. 1062. [42 U.S.C. § 2000ee-1]

(a) **DESIGNATION AND FUNCTIONS.**—The Attorney General, the Secretary of Defense, the Secretary of State, the Secretary of the Treasury, the Secretary of Health and Human Services, the Secretary of Homeland Security, the Director of National Intelligence, the Director of the Central Intelligence Agency, the Director of the National Security Agency, the Director of the Federal Bureau of Investigation, and the head of any other department, agency, or element of the executive branch designated by the Privacy and Civil Liberties Oversight Board under section 1061 to be appropriate for coverage under this section shall designate not less than 1 senior officer to serve as the principal advisor to—

- (1) assist the head of such department, agency, or element and other officials of such department, agency, or element in appropriately considering privacy and civil liberties concerns when such officials are proposing, developing, or implementing laws, regulations, policies, procedures, or guidelines related to efforts to protect the Nation against terrorism;
- (2) periodically investigate and review department, agency, or element actions, policies, procedures, guidelines, and related laws and their implementation to ensure that such department, agency, or element is adequately considering privacy and civil liberties in its actions;
- (3) ensure that such department, agency, or element has adequate procedures to receive, investigate, respond to, and redress complaints

from individuals who allege such department, agency, or element has violated their privacy or civil liberties; and

(4) in providing advice on proposals to retain or enhance a particular governmental power the officer shall consider whether such department, agency, or element has established—

(A) that the need for the power is balanced with the need to protect privacy and civil liberties;

(B) that there is adequate supervision of the use by such department, agency, or element of the power to ensure protection of privacy and civil liberties; and

(C) that there are adequate guidelines and oversight to properly confine its use.

(b) EXCEPTION TO DESIGNATION AUTHORITY.—

(1) PRIVACY OFFICERS.—In any department, agency, or element referred to in subsection (a) or designated by the Privacy and Civil Liberties Oversight Board, which has a statutorily created privacy officer, such officer shall perform the functions specified in subsection (a) with respect to privacy.

(2) CIVIL LIBERTIES OFFICERS.—In any department, agency, or element referred to in subsection (a) or designated by the Board, which has a statutorily created civil liberties officer, such officer shall perform the functions specified in subsection (a) with respect to civil liberties.

(c) SUPERVISION AND COORDINATION.—Each privacy officer or civil liberties officer described in subsection (a) or (b) shall—

(1) report directly to the head of the department, agency, or element concerned; and

(2) coordinate their activities with the Inspector General of such department, agency, or element to avoid duplication of effort.

(d) AGENCY COOPERATION.—The head of each department, agency, or element shall ensure that each privacy officer and civil liberties officer—

(1) has the information, material, and resources necessary to fulfill the functions of such officer;

(2) is advised of proposed policy changes;

(3) is consulted by decision makers; and

(4) is given access to material and personnel the officer determines to be necessary to carry out the functions of such officer.

(e) REPRISAL FOR MAKING COMPLAINT.—No action constituting a reprisal, or threat of reprisal, for making a complaint or for disclosing information to a privacy officer or civil liberties officer described in subsection (a) or (b), or to the Privacy and Civil Liberties Oversight Board, that indicates a possible violation of privacy protections or civil liberties in the administration of the programs and operations of the Federal Government relating to efforts to protect the Nation

from terrorism shall be taken by any Federal employee in a position to take such action, unless the complaint was made or the information was disclosed with the knowledge that it was false or with willful disregard for its truth or falsity.

(f) PERIODIC REPORTS.—

(1) IN GENERAL.—The privacy officers and civil liberties officers of each department, agency, or element referred to or described in subsection (a) or (b) shall periodically, but not less than annually, submit a report on the activities of such officers—

(A)(i) to the appropriate committees of Congress, including the Committee on the Judiciary of the Senate, the Committee on the Judiciary of the House of Representatives, the Committee on Homeland Security and Governmental Affairs of the Senate, the Committee on Oversight and Government Reform of the House of Representatives, the Select Committee on Intelligence of the Senate, and the Permanent Select Committee on Intelligence of the House of Representatives;

(ii) to the head of such department, agency, or element;
and

(iii) to the Privacy and Civil Liberties Oversight Board;
and

(B) which shall be in unclassified form to the greatest extent possible, with a classified annex where necessary.

(2) CONTENTS.—Each report submitted under paragraph (1) shall include information on the discharge of each of the functions of the officer concerned, including—

(A) information on the number and types of reviews undertaken;

(B) the type of advice provided and the response given to such advice;

(C) the number and nature of the complaints received by the department, agency, or element concerned for alleged violations;
and

(D) a summary of the disposition of such complaints, the reviews and inquiries conducted, and the impact of the activities of such officer.

(g) INFORMING THE PUBLIC.—Each privacy officer and civil liberties officer shall—

(1) make the reports of such officer, including reports to Congress, available to the public to the greatest extent that is consistent with the protection of classified information and applicable law; and

(2) otherwise inform the public of the activities of such officer, as appropriate and in a manner consistent with the protection of classified information and applicable law.

(h) SAVINGS CLAUSE.—Nothing in this section shall be construed to limit or otherwise supplant any other authorities or responsibilities provided by law to privacy officers or civil liberties officers.

TITLE III—SECURITY CLEARANCES

SECURITY CLEARANCES

SEC. 3001. [50 U.S.C. § 3341]

(a) DEFINITIONS.—In this section:

(1) The term “agency” means—

(A) an executive agency (as that term is defined in section 105 of title 5, United States Code);

(B) a military department (as that term is defined in section 102 of title 5, United States Code); or

(C) an element of the intelligence community.

(2) The term “authorized investigative agency” means an agency designated by the head of the agency selected pursuant to subsection (b) to conduct a counterintelligence investigation or investigation of persons who are proposed for access to classified information to ascertain whether such persons satisfy the criteria for obtaining and retaining access to such information.

(3) The term “authorized adjudicative agency” means an agency authorized by law, regulation, or direction of the Director of National Intelligence to determine eligibility for access to classified information in accordance with Executive Order 12968.

(4) The term “highly sensitive program” means—

(A) a government program designated as a Special Access Program (as that term is defined in section 4.1(h) of Executive Order 12958 or any successor Executive order); or

(B) a government program that applies restrictions required for—

(i) restricted data (as that term is defined in section 11 y. of the Atomic Energy Act of 1954 (42 U.S.C. 2014(y))); or

(ii) other information commonly referred to as “sensitive compartmented information”.

(5) The term “current investigation file” means, with respect to a security clearance, a file on an investigation or adjudication that has been conducted during—

- (A) the 5-year period beginning on the date the security clearance was granted, in the case of a Top Secret Clearance, or the date access was granted to a highly sensitive program;
 - (B) the 10-year period beginning on the date the security clearance was granted in the case of a Secret Clearance; and
 - (C) the 15-year period beginning on the date the security clearance was granted in the case of a Confidential Clearance.
- (6) The term “personnel security investigation” means any investigation required for the purpose of determining the eligibility of any military, civilian, or government contractor personnel to access classified information.
- (7) The term “periodic reinvestigations” means investigations conducted for the purpose of updating a previously completed background investigation—
- (A) every 5 years in the case of a top secret clearance or access to a highly sensitive program;
 - (B) every 10 years in the case of a secret clearance; or
 - (C) every 15 years in the case of a Confidential Clearance.
- (8) The term “appropriate committees of Congress” means—
- (A) the Permanent Select Committee on Intelligence and the Committees on Armed Services, Homeland Security, Government Reform, and the Judiciary of the House of Representatives; and
 - (B) the Select Committee on Intelligence and the Committees on Armed Services, Homeland Security and Governmental Affairs, and the Judiciary of the Senate.
- (9) ACCESS DETERMINATION.—The term “access determination” means the determination regarding whether an employee—
- (A) is eligible for access to classified information in accordance with Executive Order 12968 (60 Fed. Reg. 40245; relating to access to classified information), or any successor thereto, and Executive Order 10865 (25 Fed. Reg. 1583; relating to safeguarding classified information within industry), or any successor thereto; and
 - (B) possesses a need to know under such an Order.
- (b) SELECTION OF ENTITY.—Except as otherwise provided, not later than 90 days after the date of enactment of this Act, the President shall select a single department, agency, or element of the executive branch to be responsible for—
- (1) directing day-to-day oversight of investigations and adjudications for personnel security clearances, including for highly sensitive programs, throughout the United States Government;

- (2) developing and implementing uniform and consistent policies and procedures to ensure the effective, efficient, and timely completion of security clearances and determinations for access to highly sensitive programs, including the standardization of security questionnaires, financial disclosure requirements for security clearance applicants, and polygraph policies and procedures;
- (3) serving as the final authority to designate an authorized investigative agency or authorized adjudicative agency;
- (4) ensuring reciprocal recognition of access to classified information among the agencies of the United States Government, including acting as the final authority to arbitrate and resolve disputes involving the reciprocity of security clearances and access to highly sensitive programs pursuant to subsection (d);
- (5) ensuring, to the maximum extent practicable, that sufficient resources are available in each agency to achieve clearance and investigative program goals;
- (6) reviewing and coordinating the development of tools and techniques for enhancing the conduct of investigations and granting of clearances; and
- (7) not later than 180 days after the date of the enactment of the Intelligence Authorization Act for Fiscal Year 2014, and consistent with subsection (j)—
 - (A) developing policies and procedures that permit, to the extent practicable, individuals alleging reprisal for having made a protected disclosure (provided the individual does not disclose classified information or other information contrary to law) to appeal any action affecting an employee's access to classified information and to retain their government employment status while such challenge is pending; and
 - (B) developing and implementing uniform and consistent policies and procedures to ensure proper protections during the process for denying, suspending, or revoking a security clearance or access to classified information following a protected disclosure, including the ability to appeal such a denial, suspension, or revocation, except that there shall be no appeal of an agency's suspension of a security clearance or access determination for purposes of conducting an investigation, if that suspension lasts no longer than 1 year or the head of the agency or a designee of the head of the agency certifies that a longer suspension is needed before a final decision on denial or revocation to prevent imminent harm to the national security.

(c) PERFORMANCE OF SECURITY CLEARANCE INVESTIGATIONS.—

(1) Notwithstanding any other provision of law, not later than 180 days after the date of the enactment of this Act, the President shall, in consultation with the head of the entity selected pursuant to subsection (b), select a single agency of the executive branch to conduct, to the maximum extent practicable, security clearance investigations of employees and contractor personnel of the United States Government who require access to classified information and to provide and maintain all security clearances of such employees and contractor personnel. The head of the entity selected pursuant to subsection (b) may designate other agencies to conduct such investigations if the head of the entity selected pursuant to subsection (b) considers it appropriate for national security and efficiency purposes.

(2) The agency selected under paragraph (1) shall—

(A) take all necessary actions to carry out the requirements of this section, including entering into a memorandum of understanding with any agency carrying out responsibilities relating to security clearances or security clearance investigations before the date of the enactment of this Act;

(B) as soon as practicable, integrate reporting of security clearance applications, security clearance investigations, and determinations of eligibility for security clearances, with the database required by subsection (e); and

(C) ensure that security clearance investigations are conducted in accordance with uniform standards and requirements established under subsection (b), including uniform security questionnaires and financial disclosure requirements.

(d) RECIPROcity OF SECURITY CLEARANCE AND ACCESS DETERMINATIONS.—

(1) All security clearance background investigations and determinations completed by an authorized investigative agency or authorized adjudicative agency shall be accepted by all agencies.

(2) All security clearance background investigations initiated by an authorized investigative agency shall be transferable to any other authorized investigative agency.

(3)(A) An authorized investigative agency or authorized adjudicative agency may not establish additional investigative or adjudicative requirements (other than requirements for the conduct of a polygraph examination) that exceed requirements specified in Executive Orders establishing security requirements for access to classified information without the approval of the head of the entity selected pursuant to subsection (b).

(B) Notwithstanding subparagraph (A), the head of the entity selected pursuant to subsection (b) may establish such additional requirements as the head of such entity considers necessary for national security purposes.

(4) An authorized investigative agency or authorized adjudicative agency may not conduct an investigation for purposes of determining whether to grant a security clearance to an individual where a current investigation or clearance of equal level already exists or has been granted by another authorized adjudicative agency.

(5) The head of the entity selected pursuant to subsection (b) may disallow the reciprocal recognition of an individual security clearance by an agency under this section on a case-by-case basis if the head of the entity selected pursuant to subsection (b) determines that such action is necessary for national security purposes.

(6) The head of the entity selected pursuant to subsection (b) shall establish a review procedure by which agencies can seek review of actions required under this section.

(e) DATABASE ON SECURITY CLEARANCES.—

(1) Not later than 12 months after the date of the enactment of this Act, the Director of the Office of Personnel Management shall, in cooperation with the heads of the entities selected pursuant to subsections (b) and (c), establish and commence operating and maintaining an integrated, secure, database into which appropriate data relevant to the granting, denial, or revocation of a security clearance or access pertaining to military, civilian, or government contractor personnel shall be entered from all authorized investigative and adjudicative agencies.

(2) The database under this subsection shall function to integrate information from existing Federal clearance tracking systems from other authorized investigative and adjudicative agencies into a single consolidated database.

(3) Each authorized investigative or adjudicative agency shall check the database under this subsection to determine whether an individual the agency has identified as requiring a security clearance has already been granted or denied a security clearance, or has had a security clearance revoked, by any other authorized investigative or adjudicative agency.

(4) The head of the entity selected pursuant to subsection (b) shall evaluate the extent to which an agency is submitting information to, and requesting information from, the database under this subsection as part of a determination of whether to certify the agency as an authorized investigative agency or authorized adjudicative agency.

(5) The head of the entity selected pursuant to subsection (b) may authorize an agency to withhold information about certain individuals

from the database under this subsection if the head of the entity considers it necessary for national security purposes.

(f) EVALUATION OF USE OF AVAILABLE TECHNOLOGY IN CLEARANCE INVESTIGATIONS AND ADJUDICATIONS.—

(1) The head of the entity selected pursuant to subsection (b) shall evaluate the use of available information technology and databases to expedite investigative and adjudicative processes for all and to verify standard information submitted as part of an application for a security clearance.

(2) The evaluation shall assess the application of the technologies described in paragraph (1) for—

(A) granting interim clearances to applicants at the secret, top secret, and special access program levels before the completion of the appropriate full investigation;

(B) expediting investigations and adjudications of security clearances, including verification of information submitted by the applicant;

(C) ongoing verification of suitability of personnel with security clearances in effect for continued access to classified information;

(D) use of such technologies to augment periodic reinvestigations;

(E) assessing the impact of the use of such technologies on the rights of applicants to verify, correct, or challenge information obtained through such technologies; and

(F) such other purposes as the head of the entity selected pursuant to subsection (b) considers appropriate.

(3) An individual subject to verification utilizing the technology described in paragraph (1) shall be notified of such verification, shall provide consent to such use, and shall have access to data being verified in order to correct errors or challenge information the individual believes is incorrect.

(4) Not later than one year after the date of the enactment of this Act, the head of the entity selected pursuant to subsection (b) shall submit to the President and the appropriate committees of Congress a report on the results of the evaluation, including recommendations on the use of technologies described in paragraph (1).

(i) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to be appropriated such sums as may be necessary for fiscal year 2005 and each fiscal year thereafter for the implementation, maintenance, and operation of the database required by subsection (e).

(j) RETALIATORY REVOCATION OF SECURITY CLEARANCES AND ACCESS DETERMINATIONS.—

(1) IN GENERAL.—Agency personnel with authority to take, direct others to take, recommend, or approve personnel security clearance or access determinations shall not take or fail to take, or threaten to take or fail to take, any action with respect to any employee’s security clearance or access determination in retaliation for—

(A) any lawful disclosure of information to the Director of National Intelligence (or an employee designated by the Director of National Intelligence for such purpose) or a supervisor in the employee’s direct chain of command, or a supervisor of the employing agency with responsibility for the subject matter of the disclosure, up to and including, the head of the employing agency (or employee designated by the head of that agency for such purpose) by an employee that the employee reasonably believes evidences—

- (i) a violation of any Federal law, rule, or regulation; or
- (ii) mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety;

(B) any lawful disclosure to the Inspector General of an agency or another employee designated by the head of the agency to receive such disclosures, of information which the employee reasonably believes evidences—

- (i) a violation of any Federal law, rule, or regulation; or
- (ii) mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety;

(C) any lawful disclosure that complies with—

- (i) subsections (a)(1), (d), and (h) of section 8H of the Inspector General Act of 1978 (5 U.S.C. App.);
- (ii) subparagraphs (A), (D), and (H) of section 17(d)(5) of the Central Intelligence Agency Act of 1949 (50 U.S.C. 3517(d)(5)); or
- (iii) subparagraphs (A), (D), and (I) of section 103(k)(5) of the National Security Act of 1947 (50 U.S.C. 3033(k)(5)); and

(D) if the actions do not result in the employee or applicant unlawfully disclosing information specifically required by Executive order to be kept classified in the interest of national

defense or the conduct of foreign affairs, any lawful disclosure in conjunction with—

- (i) the exercise of any appeal, complaint, or grievance right granted by any law, rule, or regulation;
- (ii) testimony for or otherwise lawfully assisting any individual in the exercise of any right referred to in clause (i); or
- (iii) cooperation with or disclosing information to the Inspector General of an agency, in accordance with applicable provisions of law in connection with an audit, inspection, or investigation conducted by the Inspector General.

(2) **RULE OF CONSTRUCTION.**—Consistent with the protection of sources and methods, nothing in paragraph (1) shall be construed to authorize the withholding of information from Congress or the taking of any personnel action or clearance action against an employee who lawfully discloses information to Congress.

(3) **DISCLOSURES.** —A disclosure shall not be excluded from paragraph (1) because—

- (A) the disclosure was made to a person, including a supervisor, who participated in an activity that the employee reasonably believed to be covered by paragraph (1)(A)(ii);
- (B) the disclosure revealed information that had been previously disclosed;
- (C) the disclosure was not made in writing;
- (D) the disclosure was made while the employee was off duty;
- (E) of the amount of time which has passed since the occurrence of the events described in the disclosure; or
- (F) the disclosure was made during the normal course of duties of an employee.

(4) **AGENCY ADJUDICATION.**—

(A) **REMEDIAL PROCEDURE.**—An employee or former employee who believes that he or she has been subjected to a reprisal prohibited by paragraph (1) may, within 90 days (except as provided by subparagraph (D) after the issuance of notice of such decision, appeal that decision within the agency of that employee or former employee through proceedings authorized by subsection (b)(7), except that there shall be no appeal of an agency's suspension of a security clearance or access determination for purposes of conducting an investigation, if that suspension lasts not longer than 1 year (or a longer period in accordance with a certification made under subsection (b)(7)).

(B) CORRECTIVE ACTION.—If, in the course of proceedings authorized under subparagraph (A), it is determined that the adverse security clearance or access determination violated paragraph (1), the agency shall take specific corrective action to return the employee or former employee, as nearly as practicable and reasonable, to the position such employee or former employee would have held had the violation not occurred. Such corrective action may include back pay and related benefits, travel expenses, and compensatory damages not to exceed \$300,000.

(C) CONTRIBUTING FACTOR.—In determining whether the adverse security clearance or access determination violated paragraph (1), the agency shall find that paragraph (1) was violated if a disclosure described in paragraph (1) was a contributing factor in the adverse security clearance or access determination taken against the individual, unless the agency demonstrates by a preponderance of the evidence that it would have taken the same action in the absence of such disclosure, giving the utmost deference to the agency’s assessment of the particular threat to the national security interests of the United States in the instant matter.

(D) TOLLING. —The time requirement established by subparagraph (A) for an employee or former employee to appeal the decision of an agency may be tolled if the employee or former employee presents substantial credible evidence showing why the employee or former employee did not timely initiate the appeal and why the enforcement of the time requirement would be unfair, such as evidence showing that the employee or former employee—

- (i) did not receive notice of the decision; or
- (ii) could not timely initiate the appeal because of factors beyond the control of the employee or former employee.

(5) APPELLATE REVIEW OF SECURITY CLEARANCE ACCESS DETERMINATIONS BY DIRECTOR OF NATIONAL INTELLIGENCE.—

(A) APPEAL.—Within 60 days after receiving notice of an adverse final agency determination under a proceeding under paragraph (4), an employee or former employee may appeal that determination in accordance with the procedures established under subparagraph (B).

(B) POLICIES AND PROCEDURES.—The Director of National Intelligence, in consultation with the Attorney General and the Secretary of Defense, shall develop and implement policies and

procedures for adjudicating the appeals authorized by subparagraph (A).

(C) CONGRESSIONAL NOTIFICATION.—Consistent with the protection of sources and methods, at the time the Director of National Intelligence issues an order regarding an appeal pursuant to the policies and procedures established by this paragraph, the Director of National Intelligence shall notify the congressional intelligence committees.

(6) JUDICIAL REVIEW.—Nothing in this section shall be construed to permit or require judicial review of any—

(A) agency action under this section; or

(B) action of the appellate review procedures established under paragraph (5).

(7) PRIVATE CAUSE OF ACTION.—Nothing in this section shall be construed to permit, authorize, or require a private cause of action to challenge the merits of a security clearance determination.

(8) ENFORCEMENT. —Except as otherwise provided in this subsection, the President shall provide for the enforcement of this section consistent, to the fullest extent possible, with the policies and procedures used to adjudicate alleged violations of section 2302(b)(8) of title 5, United States Code.

(9) INCLUSION OF CONTRACTOR EMPLOYEES.—In this subsection, the term “employee” includes an employee of a contractor, subcontractor, grantee, subgrantee, or personal services contractor, of an agency. With respect to such employees, the term “employing agency” shall be deemed to be the contracting agency.

CENTRAL INTELLIGENCE AGENCY ACT OF 1949

[Public Law 110; 63 STAT. 208; June 20, 1949]

AN ACT To provide for the administration of the Central Intelligence Agency, established pursuant to section 102, National Security Act of 1947, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

TABLE OF CONTENTS¹

- SEC. 1. Definitions.
- SEC. 2. Seal of office.
- SEC. 3. Procurement authorities.
- SEC. 4. Travel, allowances and related expenses.
- SEC. 5. General authorities.
- SEC. 6. Protection of nature of Agency's functions.
- SEC. 7. Admission of essential aliens; limitation on number.
- SEC. 8. Appropriations.
- SEC. 9. Separability of provisions.
- SEC. 10. Short title.
- SEC. 11. Benefits available in event of the death of personnel.
- SEC. 12. Gifts, devises, and bequests.
- SEC. 13. Misuse of Agency name, initials, or seal.
- SEC. 14. Retirement equity for spouses of certain employees.
- SEC. 15. Security personnel at agency installations.
- SEC. 16. Heath benefits for certain former spouses of Central Intelligence Agency employees.
- SEC. 17. Inspector General for Agency.
- SEC. 17 note. Inspector General for Agency continued.
- SEC. 18. Special annuity computation rules for certain employees' service abroad.
- SEC. 19. Special rules for disability retirement and death-in-service benefits with respect to certain employees.
- SEC. 19A. Special rules for certain individuals injured by reason of war, insurgency, hostile act, terrorist activities, or incidents designated by the Director.
- SEC. 20. General Counsel of the Central Intelligence Agency.

¹ Table of Contents does not appear in the Act itself.

CENTRAL INTELLIGENCE AGENCY ACT OF 1949

- SEC. 21. Central services program.
- SEC. 22. Detail of employees.
- SEC. 23. Intelligence operations and cover enhancement authority.
- SEC. 24. Office of the Ombudsman for Analytic Objectivity.
- SEC. 25. Improvement of Education in Science, Technology, Engineering, Arts, and Mathematics.
- SEC. 26. Chaplain Corps and Chief of Chaplains.
- SEC. 27. Compensation and Professional Standards for Certain Medical Officers.
- SEC. 28. Medical Advisory Board.
- SEC. 29. Office of Wellness and Workforce Support.
- SEC. 30. Sexual assault and sexual harassment within the Agency.
- SEC. 31. Reporting and investigation of allegations of sexual assault and sexual harassment.
- SEC. 32. Special victim investigator.

50 U.S.C. § 3519a.

Separation pay program for voluntary separation from service.

DEFINITIONS

SEC. 1. [50 U.S.C. § 3501]

That when used in this Act, the term—

- (1) “Agency” means the Central Intelligence Agency;
- (2) “Director” means the Director of the Central Intelligence Agency;
- and
- (3) “Government agency” means any executive department, commission, council, independent establishment, corporation wholly or partly owned by the United States which is an instrumentality of the United States, board, bureau, division, service, office, officer, authority, administration, or other establishment, in the executive branch of the Government.

SEAL OF OFFICE

SEC. 2. [50 U.S.C. § 3502]

The Director shall cause a seal of office to be made for the Central Intelligence Agency, of such design as the President shall approve, and judicial notice shall be taken thereof.

PROCUREMENT AUTHORITIES

SEC. 3. [50 U.S.C. § 3503]

(a) In the performance of its functions the Central Intelligence Agency is authorized to exercise the authorities contained in sections 3201, 3203, 3204, 3206, 3207, 3302 through 3306, 3321 through 3323, 3801 through 3808, 3069, 3134, 3841, and 4752 of title 10, United States Code.

(b) In the exercise of the authorities granted in subsection (a) of this section, the term “Agency head” shall mean the Director, the Deputy Director, or the Executive of the Agency.

(c) The determinations and decisions provided in subsection (a) of this section to be made by the Agency head may be made with respect to individual purchases and contracts or with respect to classes of purchases or contracts, and shall be final. Except as provided in subsection (d) of this section, the Agency head is authorized to delegate his powers provided in this section, including the making of such determinations and decisions, in his discretion and subject to his direction, to any other officer or officers or officials of the Agency.

(d) The power of the Agency head to make the determinations or decisions specified in sections 3201 through 3204 of title 10 shall not be delegable. Each determination or decision required by sections 3201 through 3204, 3321 through 3323, and 3841 of title 10 shall be based upon written findings made by the official making such determinations, which findings shall be final and shall be available within the Agency for a period of at least six years following the date of the determination.

TRAVEL, ALLOWANCES AND RELATED EXPENSES

SEC. 4. [50 U.S.C. § 3505]

(a) Under such regulations as the Director may prescribe, the Agency, with respect to its officers and employees assigned to duty stations outside the several States of the United States of America, excluding Alaska and Hawaii, but including the District of Columbia, shall—

(1)(A) pay the travel expenses of officers and employees of the Agency, including expenses incurred while traveling pursuant to authorized home leave;

(B) pay the travel expenses of members of the family of an officer or employee of the Agency when proceeding to or returning from his post of duty; accompanying him on authorized home leave; or otherwise traveling in accordance with authority granted pursuant to the terms of this or any other Act;

(C) pay the cost of transporting the furniture and household and personal effects of an officer or employee of the Agency to his successive posts of duty and, on the termination of his services,

to his residence at time of appointment or to a point not more distant, or, upon retirement, to the place where he will reside; (D) pay the cost of packing and unpacking, transporting to and from a place of storage, and storing the furniture and household and personal effects of an officer or employee of the Agency, when he is absent from his post of assignment under orders, or when he is assigned to a post to which he cannot take or at which he is unable to use such furniture and household and personal effects, or when it is in the public interest or more economical to authorize storage; but in no instance shall the weight or volume of the effects stored together with the weight or volume of the effects transported exceed the maximum limitations fixed by regulations, when not otherwise fixed by law;

(E) pay the cost of packing and unpacking, transporting to and from a place of storage, and storing the furniture and household and personal effects of an officer or employee of the Agency in connection with assignment or transfer to a new post, from the date of his departure from his last post or from the date of his departure, from his place of residence in the case of a new officer or employee and for not to exceed three months after arrival at the new post, or until the establishment of residence quarters, whichever shall be shorter; and in connection with separation of an officer or employee of the Agency, the cost of packing and unpacking, transporting to and from a place of storage, and storing for a period not to exceed three months, his furniture and household and personal effects; but in no instance shall the weight or volume of the effects stored together with the weight or volume of the effects transported exceed the maximum limitations fixed by regulations, when not otherwise fixed by law;

(F) pay the travel expenses and transportation costs incident to the removal of the members of the family of an officer or employee of the Agency and his furniture and household and personal effects, including automobiles, from a post at which, because of the prevalence of disturbed conditions, there is imminent danger to life and property, and the return of such persons, furniture, and effects to such post upon the cessation of such conditions; or to such other post as may in the meantime have become the post to which such officer or employee has been assigned.

(2) Charge expenses in connection with travel of personnel, their dependents, and transportation of their household goods and personal

effects, involving a change of permanent station, to the appropriation for the fiscal year current when any part of either the travel or transportation pertaining to the transfer begins pursuant to previously issued travel and transfer orders, notwithstanding the fact that such travel or transportation may not all be effected during such fiscal year, or the travel and transfer orders may have been issued during the prior fiscal year.

(3)(A) Order to any of the several States of the United States of America (including the District of Columbia, the Commonwealth of Puerto Rico, and any territory or possession of the United States) on leave of absence each officer or employee of the Agency who was a resident of the United States (as described above) at time of employment, upon completion of two years' continuous service abroad, or as soon as possible thereafter.

(B) While in the United States (as described in paragraph (3)(A) of this subsection) on leave, the service of any officer or employee shall be available for work or duties in the Agency or elsewhere as the Director may prescribe; and the time of such work or duty shall not be counted as leave.

(C) Where an officer or employee on leave returns to the United States (as described in paragraph (3)(A) of this subsection), leave of absence granted shall be exclusive of the time actually and necessarily occupied in going to and from the United States (as so described) and such time as may be necessarily occupied in awaiting transportation.

(4) Notwithstanding the provisions of any other law, transport for or on behalf of an officer or employee of the Agency, a privately owned motor vehicle in any case in which it shall be determined that water, rail, or air transportation of the motor vehicle is necessary or expedient for all or any part of the distance between points of origin and destination, and pay the costs of such transportation. Not more than one motor vehicle of any officer or employee of the Agency may be transported under authority of this paragraph during any four-year period, except that, as a replacement for such motor vehicle, one additional motor vehicle of any such officer or employee may be so transported during such period upon approval, in advance, by the Director and upon a determination, in advance, by the Director that such replacement is necessary for reasons beyond the control of the officer or employee and is in the interest of the Government. After the expiration of a period of four years following the date of transportation under authority of this paragraph of a privately owned motor vehicle of any officer or employee who has remained in continuous service outside the several States of the United States of America, excluding Alaska and Hawaii, but including the District of Columbia, during such period, the transportation of a replacement for

such motor vehicle for such officer or employee may be authorized by the Director in accordance with this paragraph.

(5)(A) In the event of illness or injury requiring the hospitalization of an officer or full time employee of the Agency incurred while on assignment abroad, in a locality where there does not exist a suitable hospital or clinic, pay the travel expenses of such officer or employee by whatever means the Director deems appropriate and without regard to the Standardized Government Travel Regulations and section 5731 of title 5, United States Code, to the nearest locality where a suitable hospital or clinic exists and on the recovery of such officer or employee pay for the travel expenses of the return to the post of duty of such officer or employee. If the officer or employee is too ill to travel unattended, the Director may also pay the travel expenses of an attendant;

(B) Establish a first-aid station and provide for the services of a nurse at a post at which, in the opinion of the Director, sufficient personnel is employed to warrant such a station: *Provided*, That, in the opinion of the Director, it is not feasible to utilize an existing facility;

(C) In the event of illness or injury requiring hospitalization of an officer or full time employee of the Agency incurred in the line of duty while such person is assigned abroad, pay for the cost of the treatment of such illness or injury at a suitable hospital or clinic;

(D) Provide for the periodic physical examination of officers and employees of the Agency and for the cost of administering inoculation or vaccinations to such officers or employees.

(6) Pay the costs of preparing and transporting the remains of an officer or employee of the Agency or a member of his family who may die while in travel status or abroad, to his home or official station, or to such other place as the Director may determine to be the appropriate place of interment, provided that in no case shall the expense payable be greater than the amount which would have been payable had the destination been the home or official station.

(7) Pay the costs of travel of new appointees and their dependents, and the transportation of their household goods and personal effects, from places of actual residence in foreign countries at time of appointment to places of employment and return to their actual residences at the time of appointment or a point not more distant: *Provided*, That such appointees agree in writing to remain with the United States Government for a period of not less than twelve months from the time of appointment. Violation of such agreement for personal convenience of an employee or because of separation for misconduct will bar such return payments and,

if determined by the Director or his designee to be in the best interests of the United States, any money expended by the United States on account of such travel and transportation shall be considered as a debt due by the individual concerned to the United States.

(b)(1) The Director may pay to officers and employees of the Agency, and to persons detailed or assigned to the Agency from other agencies of the Government or from the Armed Forces, allowances and benefits comparable to the allowances and benefits authorized to be paid to members of the Foreign Service under chapter 9 of title I of the Foreign Service Act of 1980 (22 U.S.C. 4081 et seq.) or any other provision of law.

(2) The Director may pay allowances and benefits related to officially authorized travel, personnel and physical security activities, operational activities, and cover-related activities (whether or not such allowances and benefits are otherwise authorized under this section or any other provision of law) when payment of such allowances and benefits is necessary to meet the special requirements of work related to such activities. Payment of allowances and benefits under this paragraph shall be in accordance with regulations prescribed by the Director. Rates for allowances and benefits under this paragraph may not be set at rates in excess of those authorized by sections 5724 and 5724a of title 5, United States Code, when reimbursement is provided for relocation attributable, in whole or in part, to relocation within the United States.

(3) Notwithstanding any other provision of this section or any other provision of law relating to the officially authorized travel of Government employees, the Director, in order to reflect Agency requirements not taken into account in the formulation of Government-wide travel procedures, may by regulation—

(A) authorize the travel of officers and employees of the Agency, and of persons detailed or assigned to the Agency from other agencies of the Government or from the Armed Forces who are engaged in the performance of intelligence functions, and

(B) provide for payment for such travel, in classes of cases, as determined by the Director, in which such travel is important to the performance of intelligence functions.

(4) Members of the Armed Forces may not receive benefits under both this section and title 37, United States Code, for the same purpose. The Director and Secretary of Defense shall prescribe joint regulations to carry out the preceding sentence.

(5) Regulations, other than regulations under paragraph (1), issued pursuant to this subsection shall be submitted to the Permanent Select Committee on Intelligence of the House of Representatives and the

Select Committee on Intelligence of the Senate before such regulations take effect.

GENERAL AUTHORITIES

SEC. 5. [50 U.S.C. § 3506]

(a) IN GENERAL.—In the performance of its functions, the Central Intelligence Agency is authorized to—

(1) Transfer to and receive from other Government agencies such sums as may be approved by the Office of Management and Budget, for the performance of any of the functions or activities authorized under section 104A of the National Security Act of 1947 (50 U.S.C. [3036]), and any other Government agency is authorized to transfer to or receive from the Agency such sums without regard to any provisions of law limiting or prohibiting transfers between appropriations. Sums transferred to the Agency in accordance with this paragraph may be expended for the purposes and under the authority of this Act without regard to limitations of appropriations from which transferred;

(2) Exchange funds without regard to section 3651 of the Revised Statutes (31 U.S.C. 543);

(3) Reimburse other Government agencies for services of personnel assigned to the Agency, and such other Government agencies are authorized, without regard to provisions of law to the contrary, so to assign or detail any officer or employee for duty with the Agency;

(4) Authorize personnel designated by the Director to carry firearms to the extent necessary for the performance of the Agency's authorized functions, except that, within the United States, such authority shall be limited to the purposes of—

(A) the training of Agency personnel and other authorized persons in the use of firearms;

(B) the protection of classified materials and information;

(C) the protection of installations and property of the Agency;

(D) the protection of—

(i) current and former Agency personnel and their immediate families;

(ii) individuals nominated by the President to the position of Director (including with respect to an individual whom a President-elect (as defined in section 3(c) of the Presidential Transition Act of 1963 (3 U.S.C. 102 note) has declared an intent to nominate) and their immediate families; and

(iii) defectors and their immediate families, and other persons in the United States under Agency auspices; and

(E) with respect to the Office of the Director of National Intelligence, the protection of—

- (i) installations and property of the Office of the Director of National Intelligence;
- (ii) the Director of National Intelligence and the immediate family of the Director;
- (iii) current and former personnel of the Office of the Director of National Intelligence and their immediate families as the Director of National Intelligence may designate; and
- (iv) individuals nominated by the President to the position of Director of National Intelligence (including with respect to an individual whom a President-elect has declared an intent to nominate) and their immediate families;

(5) Make alterations, improvements, and repairs on premises rented by the Agency, and pay rent therefor;

(6) Determine and fix the minimum and maximum limits of age within which an original appointment may be made to an operational position within the Agency, notwithstanding the provision of any other law, in accordance with such criteria as the Director, in his discretion, may prescribe;

(7) Notwithstanding section 1341(a)(1) of title 31, United States Code, enter into multiyear leases for up to 15 years; and

(8) Upon approval of the Director, provide, during any fiscal year, with or without reimbursement, subsistence to any personnel assigned to an overseas location designated by the Agency as an austere location.

(b) SCOPE OF AUTHORITY FOR EXPENDITURE.—

(1) The authority to enter into a multiyear lease under subsection (a)(7) shall be subject to appropriations provided in advance for—

- (A) the entire lease; or
- (B) the first 12 months of the lease and the Government's estimated termination liability.

(2) In the case of any such lease entered into under subparagraph (B) of paragraph (1)—

- (A) such lease shall include a clause that provides that the contract shall be terminated if budget authority (as defined by section 3(2) of the Congressional Budget and Impoundment Control Act of 1974 (2 U.S.C. 622(2))) is not provided specifically for that project in an appropriations Act in advance of an obligation of funds in respect thereto;
- (B) notwithstanding section 1552 of title 31, United States Code, amounts obligated for paying termination costs with respect to

such lease shall remain available until the costs associated with termination of such lease are paid;

(C) funds available for termination liability shall remain available to satisfy rental obligations with respect to such lease in subsequent fiscal years in the event such lease is not terminated early, but only to the extent those funds are in excess of the amount of termination liability at the time of their use to satisfy such rental obligations; and

(D) funds appropriated for a fiscal year may be used to make payments on such lease, for a maximum of 12 months, beginning any time during such fiscal year.

(c) TRANSFERS FOR ACQUISITION OF LAND.—

(1) Sums appropriated or otherwise made available to the Agency for the acquisition of land that are transferred to another department or agency for that purpose shall remain available for 3 years.

(2) The Director shall submit to the Select Committee on Intelligence of the Senate and the Permanent Select Committee on Intelligence of the House of Representatives a report on the transfer of sums described in paragraph (1) each time that authority is exercised.

PROTECTION OF NATURE OF AGENCY'S FUNCTIONS

SEC. 6. [50 U.S.C. § 3507]

In the interests of the security of the foreign intelligence activities of the United States and in order further to implement section 102A(i) of the National Security Act of 1947 that the Director of National Intelligence shall be responsible for protecting intelligence sources and methods from unauthorized disclosure, the Agency shall be exempted from the provisions of sections 1 and 2, chapter 795 of the Act of August 28, 1935 (49 Stat. 956, 957; 5 U.S.C. 654), and the provisions of any other laws which require the publication or disclosure of the organization, or functions of the Agency, or of the names, official titles, salaries, or numbers of personnel employed by the Agency: *Provided*, That in furtherance of this section, the Director of the Office of Management and Budget shall make no reports to the Congress in connection with the Agency under section 607, title VI, chapter 212 of the Act of June 30, 1945, as amended (5 U.S.C. 947(b)).

[ADMISSION OF ESSENTIAL ALIENS; LIMITATION ON NUMBER]

SEC. 7. [50 U.S.C. § 3508]

Whenever the Director, the Attorney General, and the Commissioner of Immigration and Naturalization shall determine that the admission of a particular alien into the United States for permanent residence is in the interest of national

security or essential to the furtherance of the national intelligence mission, such alien and his immediate family shall be admitted to the United States for permanent residence without regard to their inadmissibility under the immigration or any other laws and regulations, or to the failure to comply with such laws and regulations pertaining to admissibility: *Provided*, That the number of aliens and members of their immediate families admitted to the United States under the authority of this section shall in no case exceed one hundred persons in any one fiscal year.

APPROPRIATIONS

SEC. 8. [50 U.S.C. § 3510]

(a) Notwithstanding any other provisions of law, sums made available to the Agency by appropriation or otherwise may be expended for purposes necessary to carry out its functions, including—

(1) personal services, including personal services without regard to limitations on types of persons to be employed, and rent at the seat of government and elsewhere; health-service program as authorized by law (5 U.S.C. [7901]); payment of death benefits in cases in which the circumstances of the death of an employee of the Agency, a detailee of the Agency or other employee of another department or agency of the Federal Government assigned to the Agency, or an individual affiliated with the Agency (as determined by the Director), is not covered by section 11, other similar provisions of Federal law, or any regulation issued by the Director providing death benefits, but that the Director determines such payment appropriate; rental of news-reporting services; purchase or rental and operation of photographic, reproduction, cryptographic, duplication, and printing machines, equipment, and devices, and radio-receiving and radio-sending equipment and devices, including telegraph and teletype equipment; purchase, maintenance, operation, repair, and hire of passenger motor vehicles, and aircraft, and vessels of all kinds; subject to policies established by the Director, transportation of officers and employees of the Agency in Government-owned automotive equipment between their domiciles and places of employment, where such personnel are engaged in work which makes such transportation necessary, and transportation in such equipment, to and from school, of children of Agency personnel who have quarters for themselves and their families at isolated stations outside the continental United States where adequate public or private transportation is not available; printing and binding; purchase, maintenance, and cleaning of firearms, including purchase, storage, and maintenance of ammunition; subject to policies established by the Director, expenses of travel in

connection with, and expenses incident to attendance at meetings of professional, technical, scientific, and other similar organizations when such attendance would be a benefit in the conduct of the work of the Agency; association and library dues; payment of premiums or costs of surety bonds for officers or employees without regard to the provisions of 61 Stat. 646; 6 U.S.C. 14; payment of claims pursuant to 28 U.S.C.; acquisition of necessary land and the clearing of such land; construction of buildings and facilities without regard to 36 Stat. 699; 40 U.S.C. 259, 267²; repair, rental, operation, and maintenance of buildings, utilities, facilities, and appurtenances; and

(2) supplies, equipment, and personnel and contractual services otherwise authorized by law and regulations, when approved by the Director.

(b) The sums made available to the Agency may be expended without regard to the provisions of law and regulations relating to the expenditure of Government funds; and for objects of a confidential, extraordinary, or emergency nature, such expenditures to be accounted for solely on the certificate of the Director and every such certificate shall be deemed a sufficient voucher for the amount therein certified.

(c) Notification.—Not later than 30 days after the date on which the Director makes a novel and significant expenditure pursuant to subsection (a), the Director shall notify the Permanent Select Committee on Intelligence of the House of Representatives, the Select Committee on Intelligence of the Senate, the Subcommittee on Defense of the Committee on Appropriations of the Senate, and the Subcommittee on Defense of the Committee on Appropriations of the House of Representatives of such expenditure.

SEPARABILITY OF PROVISIONS

SEC. 9. [50 U.S.C. § 3501 note]

If any provision of this Act or the application of such provision to any person or circumstances, is held invalid, the remainder of this Act or the application of such provision to persons or circumstances other than those as to which it is held invalid, shall not be affected thereby.

SHORT TITLE

SEC. 10. [50 U.S.C. § 3501 note]

This Act may be cited as the “Central Intelligence Agency Act of 1949”.

² Section 14 of title 6, referred to in subsec. (a)(1), was repealed by [Pub. L. 93–310, title II, §203\(1\), June 6, 1972, 86 Stat. 202.](#)

BENEFITS AVAILABLE IN EVENT OF THE DEATH OF PERSONNEL

SEC. 11. [50 U.S.C. § 3511]

(a) **AUTHORITY.**—The Director may pay death benefits substantially similar to those authorized for members of the Foreign Service pursuant to the Foreign Service Act of 1980 (22 U.S.C. 3901 et seq.) or any other provision of law. The Director may adjust the eligibility for death benefits as necessary to meet the unique requirements of the mission of the Agency.

(b) **REGULATIONS.**—Regulations issued pursuant to this section shall be submitted to the Select Committee on Intelligence of the Senate and the Permanent Select Committee on Intelligence of the House of Representatives before such regulations take effect.

GIFTS, DEVISES, AND BEQUESTS

SEC. 12. [50 U.S.C. § 3512]

(a)(1) Subject to the provisions of this section, the Director may accept, hold, administer, and use gifts of money, securities, or other property whenever the Director determines it would be in the interest of the United States to do so.

(2) Any gift accepted by the Director as a gift to the Agency under this subsection (and any income produced by any such gift)—

(A) may be used only for—

(i) artistic display;

(ii) purposes relating to the general welfare, education, or recreation of employees or dependents of employees of the Agency or for similar purposes; or

(iii) purposes relating to the welfare, education, or recreation of an individual described in paragraph (3); and

(B) under no circumstances may such a gift (or any income produced by any such gift) be used for operational purposes.

(3) An individual described in this paragraph is an individual who—

(A) is an employee or a former employee of the Agency who suffered injury or illness while employed by the Agency that—

(i) resulted from hostile or terrorist activities;

(ii) occurred in connection with an intelligence activity having a significant element of risk; or

(iii) occurred under other circumstances determined by the Director to be analogous to the circumstances described in clause (i) or (ii);

(B) is a family member of such an employee or former employee; or

(C) is a surviving family member of an employee of the Agency who died in circumstances described in clause (i), (ii), or (iii) of subparagraph (A).

(4) The Director may not accept any gift under this section that is expressly conditioned upon any expenditure not to be met from the gift itself or from income produced by the gift unless such expenditure has been authorized by law.

(5) The Director may, in the Director's discretion, determine that an individual described in subparagraph (A) or (B) of paragraph (3) may accept a gift for the purposes described in paragraph (2)(A)(iii).

(b) Unless otherwise restricted by the terms of the gift, the Director may sell or exchange, or invest or reinvest, any property which is accepted under subsection (a), but any such investment may only be in interest-bearing obligations of the United States or in obligations guaranteed as to both principal and interest by the United States.

(c) There is hereby created on the books of the Treasury of the United States a fund into which gifts of money, securities, and other intangible property accepted under the authority of subsection (a), and the earnings and proceeds thereof, shall be deposited. The assets of such fund shall be disbursed upon the order of the Director for the purposes specified in subsection (a) or (b).

(d) For purposes of Federal income, estate, and gift taxes, gifts accepted by the Director under subsection (a) shall be considered to be to or for the use of the United States.

(e) For the purposes of this section, the term "gift" includes a bequest or devise.

(f)(1) The Director may engage in fundraising in an official capacity for the benefit of nonprofit organizations that provide support to surviving family members of deceased Agency employees or that otherwise provide support for the welfare, education, or recreation of Agency employees, former Agency employees, or their family members.

(2) In this subsection, the term "fundraising" means the raising of funds through the active participation in the promotion, production, or presentation of an event designed to raise funds and does not include the direct solicitation of money by any other means.

(3) Not later than the date that is 7 days after the date the Director engages in fundraising authorized by this subsection or at the time the decision is made to participate in such fundraising, the Director shall notify the Select Committee on Intelligence of the Senate and the Permanent Select Committee on Intelligence of the House of Representatives of the fundraising.

(g) The Director, in consultation with the Director of the Office of Government Ethics, shall issue regulations to carry out the authority provided in this section.

Such regulations shall ensure that such authority is exercised consistent with all relevant ethical constraints and principles, including—

- (1) the avoidance of any prohibited conflict of interest or appearance of impropriety; and
- (2) a prohibition against the acceptance of a gift from a foreign government or an agent of a foreign government.

MISUSE OF AGENCY NAME, INITIALS, OR SEAL

SEC. 13. [50 U.S.C. § 3513]

(a) No person may, except with the written permission of the Director, knowingly use the words “Central Intelligence Agency”, the initials “CIA”, the seal of the Central Intelligence Agency, or any colorable imitation of such words, initials, or seal in connection with any merchandise, impersonation, solicitation, or commercial activity in a manner reasonably calculated to convey the impression that such use is approved, endorsed, or authorized by the Central Intelligence Agency.

(b) Whenever it appears to the Attorney General that any person is engaged or is about to engage in an act or practice which constitutes or will constitute conduct prohibited by subsection (a), the Attorney General may initiate a civil proceeding in a district court of the United States to enjoin such act or practice. Such court shall proceed as soon as practicable to the hearing and determination of such action and may, at any time before final determination, enter such restraining orders or prohibitions, or take such other action as is warranted, to prevent injury to the United States or to any person or class of persons for whose protection the action is brought.

RETIREMENT EQUITY FOR SPOUSES OF CERTAIN EMPLOYEES

SEC. 14. [50 U.S.C. § 3514]

(a) The provisions of sections 102, 221(b)(1)-(3), 221(f), 221(g), 221(i)(2), 221(j), 221(m), 222, 223, 224, 225, 232(b), 241(b), 241(d) and 264(b) of the Central Intelligence Agency Retirement Act (50 U.S.C. 403 note) establishing certain requirements, limitations, rights, entitlements, and benefits relating to retirement annuities, survivor benefits, and lump-sum payments for a spouse or former spouse of an Agency employee who is a participant in the Central Intelligence Agency Retirement and Disability System shall apply in the same manner and to the same extent in the case of an Agency employee who is a participant in the Civil Service Retirement and Disability System.

(b) The Director of the Office of Personnel Management, in consultation with the Director of the Central Intelligence Agency, shall prescribe such regulations as may be necessary to implement the provisions of this section.

SECURITY PERSONNEL AT AGENCY INSTALLATIONS

SEC. 15. [50 U.S.C. § 3515]

(a)(1) The Director may authorize Agency personnel within the United States to perform the same functions as officers and agents of the Department of Homeland Security, as provided in section 1315(b)(2) of title 40, United States Code, with the powers set forth in that section, except that such personnel shall perform such functions and exercise such powers—

(A) within the Agency Headquarters Compound and the property controlled and occupied by the Federal Highway Administration located immediately adjacent to such Compound;

(B) in the streets, sidewalks, and the open areas within the zone beginning at the outside boundary of such Compound and property and extending outward 500 yards;

(C) within any other Agency installation and protected property;

(D) within an installation owned, or contracted to be occupied for a period of one year or longer, by the Office of the Director of National Intelligence; and

(E) in the streets, sidewalks, and open areas within the zone beginning at the outside boundary of any installation or property referred to in subparagraph (C) or (D) and extending outward 500 yards.

(2) The performance of functions and exercise of powers under subparagraph (B) or (E) of paragraph (1) shall be limited to those circumstances where such personnel can identify specific and articulable facts giving such personnel reason to believe that the performance of such functions and exercise of such powers is reasonable to protect against physical damage or injury, or threats of physical damage or injury, to Agency installations, property, or employees.

(3) Nothing in this subsection shall be construed to preclude, or limit in any way, the authority of any Federal, State, or local law enforcement agency, or any other Federal police or Federal protective service.

(4) The rules and regulations enforced by such personnel shall be the rules and regulations prescribed by the Director and shall only be applicable to the areas referred to in subparagraph (A),(C), or (D) of paragraph (1).

(b) The Director is authorized to establish penalties for violations of the rules or regulations promulgated by the Director under subsection (a) of this section. Such penalties shall not exceed the maximum penalty authorized for a Class B misdemeanor under section 3559 of title 18, United States Code.

(c) Agency personnel designated by the Director under subsection (a) of this section shall be clearly identifiable as United States Government security

personnel while engaged in the performance of the functions to which subsection (a) of this section refers.

(d)(1) Notwithstanding any other provision of law, any Agency personnel designated by the Director under subsection (a) of this section, or designated by the Director to carry firearms under subparagraph (D) or (E) of section 5(a)(4), shall be considered for purposes of chapter 171 of title 28, United States Code, or any other provision of law relating to tort liability, to be acting within the scope of their office or employment when such Agency personnel take reasonable action, which may include the use of force, to—

(A) protect an individual in the presence of such Agency personnel from a crime of violence;

(B) provide immediate assistance to an individual who has suffered or who is threatened with bodily harm; or

(C) prevent the escape of any individual whom such Agency personnel reasonably believe to have committed a crime of violence in the presence of such Agency personnel.

(2) Paragraph (1) shall not affect the authorities of the Attorney General under section 2679 of title 28, United States Code.

(3) In this subsection, the term “crime of violence” has the meaning given that term in section 16 of title 18, United States Code.

HEALTH BENEFITS FOR CERTAIN FORMER SPOUSES OF CENTRAL INTELLIGENCE AGENCY EMPLOYEES

SEC. 16. [50 U.S.C. § 3516]

(a) Except as provided in subsection (e), any individual —

(1) formerly married to an employee or former employee of the Agency, whose marriage was dissolved by divorce or annulment before May 7, 1985;

(2) who, at any time during the eighteen-month period before the divorce or annulment became final, was covered under a health benefits plan as a member of the family of such employee or former employee; and

(3) who was married to such employee for not less than ten years during periods of service by such employee with the Agency, at least five years of which were spent outside the United States by both the employee and the former spouse,

is eligible for coverage under a health benefits plan in accordance with the provisions of this section.

(b)(1) Any individual eligible for coverage under subsection (a) may enroll in a health benefits plan for self alone or for self and family if, before the expiration of the six-month period beginning on October 1, 1986, and in accordance with

such procedures as the Director of the Office of Personnel Management shall by regulation prescribe, such individual—

- (A) files an election for such enrollment; and
- (B) arranges to pay currently into the Employees Health Benefits Fund under section 8909 of title 5, United States Code, an amount equal to the sum of the employee and agency contributions payable in the case of an employee enrolled under chapter 89 of such title in the same health benefits plan and with the same level of benefits.

(2) The Director of the Central Intelligence Agency shall, as soon as possible, take all steps practicable—

- (A) to determine the identity and current address of each former spouse eligible for coverage under subsection (a); and
- (B) to notify each such former spouse of that individual's rights under this section.

(3) The Director of the Office of Personnel Management, upon notification by the Director of the Central Intelligence Agency, shall waive the six-month limitation set forth in paragraph (1) in any case in which the Director of the Central Intelligence Agency determines that the circumstances so warrant.

(c) ELIGIBILITY OF FORMER WIVES OR HUSBANDS.—

(1) Notwithstanding subsections (a) and (b) and except as provided in subsections (d), (e), and (f), an individual—

- (A) who was divorced on or before December 4, 1991, from a participant or retired participant in the Central Intelligence Agency Retirement and Disability System or the Federal Employees Retirement System Special Category;
- (B) who was married to such participant for not less than ten years during the participant's creditable service, at least five years of which were spent by the participant during the participant's service as an employee of the Agency outside the United States, or otherwise in a position the duties of which qualified the participant for designation by the Director as a participant under section 203 of the Central Intelligence Agency Retirement Act (50 U.S.C. 2013); and
- (C) who was enrolled in a health benefits plan as a family member at any time during the 18-month period before the date of dissolution of the marriage to such participant;

is eligible for coverage under a health benefits plan.

(2) A former spouse eligible for coverage under paragraph (1) may enroll in a health benefits plan in accordance with subsection (b)(1), except that the election for such enrollment must be submitted within 60 days after

the date on which the Director notifies the former spouse of such individual's eligibility for health insurance coverage under this subsection.

(d) CONTINUATION OF ELIGIBILITY.—Notwithstanding subsections (a), (b), and (c) and except as provided in subsections (e) and (f), an individual divorced on or before December 4, 1991, from a participant or retired participant in the Central Intelligence Agency Retirement and Disability System or Federal Employees' Retirement System Special Category who enrolled in a health benefits plan following the dissolution of the marriage to such participant may continue enrollment following the death of such participant notwithstanding the termination of the retirement annuity of such individual.

(e)(1) Any former spouse who remarries before age fifty-five is not eligible to make an election under subsection (b)(1).

(2) Any former spouse enrolled in a health benefits plan pursuant to an election under subsection (b)(1) or to subsection (d) may continue the enrollment under the conditions of eligibility which the Director of the Office of Personnel Management shall by regulation prescribe, except that any former spouse who remarries before age fifty-five shall not be eligible for continued enrollment under this section after the end of the thirty-one-day period beginning on the date of remarriage.

(3)(A) A former spouse who is not eligible to enroll or to continue enrollment in a health benefits plan under this section solely because of remarriage before age fifty-five shall be restored to such eligibility on the date such remarriage is dissolved by death, annulment, or divorce.

(B) A former spouse whose eligibility is restored under subparagraph (A) may, under regulations which the Director of the Office of Personnel Management shall prescribe, enroll in a health benefits plan if such former spouse—

(i) was an individual referred to in paragraph (1) and was an individual covered under a benefits plan as a family member at any time during the 18-month period before the date of dissolution of the marriage to the Agency employee or annuitant; or

(ii) was an individual referred to in paragraph (2) and was an individual covered under a benefits plan immediately before the remarriage ended the enrollment.

(f) No individual may be covered by a health benefits plan under this section during any period in which such individual is enrolled in a health benefits plan under any other authority, nor may any individual be covered under more than one enrollment under this section.

(g) For purposes of this section the term "health benefits plan" means an approved health benefits plan under chapter 89 of title 5, United States Code.

INSPECTOR GENERAL FOR AGENCY

SEC. 17. [50 U.S.C. § 3517]

(a) **PURPOSE; ESTABLISHMENT.**—In order to—

- (1) create an objective and effective office, appropriately accountable to Congress, to initiate and conduct independently inspections, investigations, and audits relating to programs and operations of the Agency;
- (2) provide leadership and recommend policies designed to promote economy, efficiency, and effectiveness in the administration of such programs and operations, and detect fraud and abuse in such programs and operations;
- (3) provide a means for keeping the Director fully and currently informed about problems and deficiencies relating to the administration of such programs and operations, and the necessity for and the progress of corrective actions; and
- (4) in the manner prescribed by this section, ensure that the Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence (hereafter in this section referred to collectively as the “intelligence committees”) are kept similarly informed of significant problems and deficiencies as well as the necessity for and the progress of corrective actions,

there is hereby established in the Agency an Office of Inspector General (hereafter in this section referred to as the “Office”).

(b) **APPOINTMENT; SUPERVISION; REMOVAL.**—

- (1) There shall be at the head of the Office an Inspector General who shall be appointed by the President, by and with the advice and consent of the Senate. This appointment shall be made without regard to political affiliation and shall be on the basis of integrity and demonstrated ability in accounting, auditing, financial analysis, law, management analysis, public administration, or investigation. Such appointment shall also be made on the basis of compliance with the security standards of the Agency and prior experience in the field of foreign intelligence.
- (2) The Inspector General shall report directly to and be under the general supervision of the Director.
- (3) The Director may prohibit the Inspector General from initiating, carrying out, or completing any audit, inspection, or investigation, or from issuing any subpoena, after the Inspector General has decided to initiate, carry out, or complete such audit, inspection, or investigation or to issue such subpoena, if the Director determines that such prohibition is necessary to protect vital national security interests of the United States.

(4) If the Director exercises any power under paragraph (3), he shall submit an appropriately classified statement of the reasons for the exercise of such power within seven days to the intelligence committees. The Director shall advise the Inspector General at the time such report is submitted, and, to the extent consistent with the protection of intelligence sources and methods, provide the Inspector General with a copy of any such report. In such cases, the Inspector General may submit such comments to the intelligence committees that he considers appropriate.

(5) In accordance with section 535 of title 28, United States Code, the Inspector General shall report to the Attorney General any information, allegation, or complaint received by the Inspector General relating to violations of Federal criminal law that involve a program or operation of the Agency, consistent with such guidelines as may be issued by the Attorney General pursuant to subsection (b)(2) of such section. A copy of all such reports shall be furnished to the Director.

(6) (A) The Inspector General may be removed from office only by the President. The President shall communicate in writing to the intelligence committees the substantive rationale, including detailed and case-specific reasons, for any such removal not later than 30 days prior to the effective date of such removal. Nothing in this paragraph shall be construed to prohibit a personnel action otherwise authorized by law, other than transfer or removal.

(B) If there is an open or completed inquiry into the Inspector General that relates to the removal or transfer of the Inspector General under subparagraph (A), the written communication required under that subparagraph shall—

- (i) identify each entity that is conducting, or that conducted, the inquiry; and
- (ii) in the case of a completed inquiry, contain the findings made during the inquiry.

(7) (A) Subject to the other provisions of this paragraph, only the President may place the Inspector General on nonduty status.

(B) If the President places the Inspector General on nonduty status, the President shall communicate in writing the substantive rationale, including detailed and case-specific reasons, for the change in status to the congressional intelligence committees not later than 15 days before the date on which the change in status takes effect, except that the President may submit that communication not later than the date on which the change in status takes effect if—

- (i) the President has made a determination that the continued presence of the Inspector General in the

workplace poses a threat described in any of clauses (i) through (iv) of section 6329b(b)(2)(A) of title 5; and (ii) in the communication, the President includes a report on the determination described in clause (i), which shall include—

- (I) a specification of which clause of section 6329b(b)(2)(A) of title 5 the President has determined applies under clause (i);
- (II) the substantive rationale, including detailed and case-specific reasons, for the determination made under clause (i);
- (III) an identification of each entity that is conducting, or that conducted, any inquiry upon which the determination under clause (i) was made; and
- (IV) in the case of an inquiry described in subclause (III) that is completed, the findings made during that inquiry.

(C) The President may not place the Inspector General on non-duty [1] status during the 30-day period preceding the date on which the Inspector General is removed or transferred under paragraph (6)(A) unless the President—

- (i) has made a determination that the continued presence of the Inspector General in the workplace poses a threat described in any of clauses (i) through (iv) of section 6329b(b)(2)(A) of title 5; and
- (ii) not later than the date on which the change in status takes effect, submits to the congressional intelligence committees a written communication that contains the information required under subparagraph (B), including the report required under clause (ii) of that subparagraph.

(8) (A) In this subsection, the term “first assistant to the position of Inspector General” has the meaning given in section 3 of the Inspector General Act of 1978 (5 U.S.C. App.).

(B) If the Inspector General dies, resigns, or is otherwise unable to perform the functions and duties of the position—

- (i) section 3345(a) of title 5 shall not apply;
- (ii) subject to subparagraph (D), the first assistant to the position of Inspector General shall perform the functions and duties of the Inspector General

temporarily in an acting capacity subject to the time limitations of section 3346 of title 5; and (iii) notwithstanding clause (ii), and subject to subparagraphs (D) and (E), the President (and only the President) may direct an officer or employee of any Office of an Inspector General to perform the functions and duties of the Inspector General temporarily in an acting capacity subject to the time limitations of section 3346 of title 5, only if—

(I) during the 365-day period preceding the date of death, resignation, or beginning of inability to serve of the Inspector General, the officer or employee served in a position in an Office of an Inspector General for not less than 90 days, except that—

(aa) the requirement under this subclause shall not apply if the officer is an Inspector General; and

(bb) for the purposes of this clause, performing the functions and duties of an Inspector General temporarily in an acting capacity does not qualify as service in a position in an Office of an Inspector General;

(II) the rate of pay for the position of the officer or employee described in subclause (I) is equal to or greater than the minimum rate of pay payable for a position at GS-15 of the General Schedule;

(III) the officer or employee has demonstrated ability in accounting, auditing, financial analysis, law, management analysis, public administration, or investigations; and

(IV) not later than 30 days before the date on which the direction takes effect, the President communicates in writing to the congressional intelligence committees the substantive rationale, including the detailed and case-specific reasons, for such direction, including the reason for the direction that someone other than the individual who is performing the functions and duties of the Inspector General

temporarily in an acting capacity (as of the date on which the President issues that direction) perform those functions and duties temporarily in an acting capacity.

(C) Notwithstanding section 3345(a) of title 5 and clauses (ii) and (iii) of subparagraph (B), and subject to subparagraph (D), during any period in which the Inspector General is on nonduty status—

- (i) the first assistant to the position of Inspector General shall perform the functions and duties of the position temporarily in an acting capacity subject to the time limitations of section 3346 of title 5; and
- (ii) if the first assistant described in clause (i) dies, resigns, or becomes otherwise unable to perform those functions and duties, the President (and only the President) may direct an officer or employee in the Office of Inspector General to perform those functions and duties temporarily in an acting capacity, subject to the time limitations of section 3346 of title 5, if—

- (I) that direction satisfies the requirements under subclauses (II), (III), and (IV) of subparagraph (B)(iii); and

- (II) that officer or employee served in a position in that Office of Inspector General for not fewer than 90 of the 365 days preceding the date on which the President makes that direction.

(D) An individual may perform the functions and duties of the Inspector General temporarily and in an acting capacity under clause (ii) or (iii) of subparagraph (B), or under subparagraph (C), with respect to only 1 Inspector General position at any given time.

(E) If the President makes a direction under subparagraph (B)(iii), during the 30-day period preceding the date on which the direction of the President takes effect, the functions and duties of the position of the Inspector General shall be performed by—

- (i) the first assistant to the position of Inspector General; or
- (ii) the individual performing those functions and duties temporarily in an acting capacity, as of the date on which the President issues that direction, if that individual is an

individual other than the first assistant to the position of Inspector General.

(c) DUTIES AND RESPONSIBILITIES.—It shall be the duty and responsibility of the Inspector General appointed under this section—

- (1) to provide policy direction for, and to plan, conduct, supervise, and coordinate independently, the inspections, investigations, and audits relating to the programs and operations of the Agency to ensure they are conducted efficiently and in accordance with applicable law and regulations;
- (2) to keep the Director fully and currently informed concerning violations of law and regulations, fraud and other serious problems, abuses and deficiencies that may occur in such programs and operations, and to report the progress made in implementing corrective action;
- (3) to take due regard for the protection of intelligence sources and methods in the preparation of all reports issued by the Office, and, to the extent consistent with the purpose and objective of such reports, take such measures as may be appropriate to minimize the disclosure of intelligence sources and methods described in such reports; and
- (4) in the execution of his responsibilities, to comply with generally accepted government auditing standards.

(d) SEMIANNUAL REPORTS; IMMEDIATE REPORTS OF SERIOUS OR FLAGRANT PROBLEMS; REPORTS OF FUNCTIONAL PROBLEMS; REPORTS TO CONGRESS ON URGENT CONCERNS.—

(1) The Inspector General shall, not later than October 31 and April 30 of each year, prepare and submit to the Director a classified semiannual report summarizing the activities of the Office during the immediately preceding six-month periods ending September 30 and March 31, respectively. Not later than 30 days after the date of the receipt of such reports, the Director shall transmit such reports to the intelligence committees with any comments he may deem appropriate. Such reports shall, at a minimum, include a list of the title or subject of each inspection, investigation, review, or audit conducted during the reporting period and—

- (A) a description of significant problems, abuses, and deficiencies relating to the administration of programs and operations of the Agency identified by the Office during the reporting period;
- (B) a description of the recommendations for corrective action made by the Office during the reporting period with respect to significant problems, abuses, or deficiencies identified in subparagraph (A);

- (C) a statement of whether corrective action has been completed on each significant recommendation described in previous semiannual reports, and, in a case where corrective action has been completed, a description of such corrective action;
- (D) a certification that the Inspector General has had full and direct access to all information relevant to the performance of his functions;
- (E) a description of the exercise of the subpoena authority under subsection (e)(5) by the Inspector General during the reporting period; and
- (F) such recommendations as the Inspector General may wish to make concerning legislation to promote economy and efficiency in the administration of programs and operations undertaken by the Agency, and to detect and eliminate fraud and abuse in such programs and operations.

(2) The Inspector General shall report immediately to the Director whenever he becomes aware of particularly serious or flagrant problems, abuses, or deficiencies relating to the administration of programs or operations. The Director shall transmit such report to the intelligence committees within seven calendar days, together with any comments he considers appropriate.

(3) In the event that—

- (A) the Inspector General is unable to resolve any differences with the Director affecting the execution of the Inspector General's duties or responsibilities;
- (B) an investigation, inspection, or audit carried out by the Inspector General should focus on any current or former Agency official who—
 - (i) holds or held a position in the Agency that is subject to appointment by the President, by and with the advice and consent of the Senate, including such a position held on an acting basis; or
 - (ii) holds or held the position in the Agency, including such a position held on an acting basis, of—
 - (I) Deputy Director;
 - (II) Associate Deputy Director;
 - (III) Director of the National Clandestine Service;
 - (IV) Director of Intelligence;
 - (V) Director of Support; or
 - (VI) Director of Science and Technology.

(C) a matter requires a report by the Inspector General to the Department of Justice on possible criminal conduct by a current or former Agency official described or referred to in subparagraph (B);

(D) the Inspector General receives notice from the Department of Justice declining or approving prosecution of possible criminal conduct of any of the officials described in subparagraph (B); or

(E) the Inspector General, after exhausting all possible alternatives, is unable to obtain significant documentary information in the course of an investigation, inspection, or audit,

the Inspector General shall immediately notify and submit a report on such matter to the intelligence committees.

(4) Pursuant to Title V of the National Security Act of 1947, the Director shall submit to the intelligence committees any report or findings and recommendations of an inspection, investigation, or audit conducted by the office which has been requested by the Chairman or Ranking Minority Member of either committee.

(5)(A) An employee of the Agency, or of a contractor to the Agency, who intends to report to Congress a complaint or information with respect to an urgent concern may report such complaint or information to the Inspector General.

(B)(i) Not later than the end of the 14-calendar day period beginning on the date of receipt from an employee of a complaint or information under subparagraph (A), the Inspector General shall determine whether the complaint or information appears credible. Upon making such a determination, the Inspector General shall transmit to the Director notice of that determination, together with the complaint or information.

(ii) If the Director determines that a complaint or information transmitted under paragraph (1) would create a conflict of interest for the Director, the Director shall return the complaint or information to the Inspector General with that determination and the Inspector General shall make the transmission to the Director of National Intelligence. In such a case, the requirements of this subsection for the Director of the Central Intelligence Agency apply to the Director of National Intelligence.

(C) Upon receipt of a transmittal from the Inspector General under subparagraph (B), the Director shall, within 7 calendar

days of such receipt, forward such transmittal to the intelligence committees, together with any comments the Director considers appropriate.

(D)(i) If the Inspector General does not find credible under subparagraph (B) a complaint or information submitted under subparagraph (A), or does not transmit the complaint or information to the Director in accurate form under subparagraph (B), the employee (subject to clause (ii)) may submit the complaint or information to Congress by contacting either or both of the intelligence committees directly.

(ii) The employee may contact the intelligence committees directly as described in clause (i) only if the employee—

(I) before making such a contact, furnishes to the Director, through the Inspector General, a statement of the employee's complaint or information and notice of the employee's intent to contact the intelligence committees directly; and

(II) obtains and follows from the Director, through the Inspector General, direction on how to contact the intelligence committees in accordance with appropriate security practices.

(iii) A member or employee of one of the intelligence committees who receives a complaint or information under clause (i) does so in that member or employee's official capacity as a member or employee of that committee.

(E) The Inspector General shall notify an employee who reports a complaint or information to the Inspector General under this paragraph of each action taken under this paragraph with respect to the complaint or information. Such notice shall be provided not later than 3 days after any such action is taken.

(F) An action taken by the Director or the Inspector General under this paragraph shall not be subject to judicial review.

(G) (i) In this paragraph:

(I) The term "urgent concern" means any of the following:

(aa) A serious or flagrant problem, abuse, violation of law or Executive order, or deficiency relating to the funding, administration, or operations of

an intelligence activity of the Federal Government that is—

(AA) a matter of national security; and

(BB) not a difference of opinion concerning public policy matters..

(bb) A false statement to Congress, or a willful withholding from Congress, on an issue of material fact relating to the funding, administration, or operation of an intelligence activity.

(cc) An action, including a personnel action described in section 2302(a)(2)(A) of title 5, United States Code, constituting reprisal or threat of reprisal prohibited under subsection (e)(3)(B) in response to an employee's reporting an urgent concern in accordance with this paragraph.

(II) The term "intelligence committees" means the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate.

(ii) Within the executive branch, the Inspector General shall have sole authority to determine whether any complaint or information reported to the Inspector General is a matter of urgent concern under this paragraph.

(H) An individual who has submitted a complaint or information to the Inspector General under this section may notify any member of the Permanent Select Committee on Intelligence of the House of Representatives or the Select Committee on Intelligence of the Senate, or a staff member of either such Committee, of the fact that such individual has made a submission to the Inspector General, and of the date on which such submission was made.

(e) AUTHORITIES OF THE INSPECTOR GENERAL.—

(1) The Inspector General shall have direct and prompt access to the Director when necessary for any purpose pertaining to the performance of his duties.

(2) The Inspector General shall have access to any employee or any employee of a contractor of the Agency whose testimony is needed for the performance of his duties. In addition, he shall have direct access to all records, reports, audits, reviews, documents, papers, recommendations, or other material which relate to the programs and operations with respect to which the Inspector General has responsibilities under this section. Failure on the part of any employee or contractor to cooperate with the Inspector General shall be grounds for appropriate administrative actions by the Director, to include loss of employment or the termination of an existing contractual relationship.

(3) The Inspector General is authorized to receive and investigate complaints or information from any person concerning the existence of an activity constituting a violation of laws, rules, or regulations, or mismanagement, gross waste of funds, abuse of authority, or a substantial and specific danger to the public health and safety. Once such complaint or information has been received from an employee of the Agency—

- (A) the Inspector General shall not disclose the identity of the employee without the consent of the employee, unless the Inspector General determines that such disclosure is unavoidable during the course of the investigation or the disclosure is made to an official of the Department of Justice responsible for determining whether a prosecution should be undertaken; and
- (B) no action constituting a reprisal, or threat of reprisal, for making such complaint or providing such information may be taken by any employee of the Agency in a position to take such actions, unless the complaint was made or the information was disclosed with the knowledge that it was false or with willful disregard for its truth or falsity.

(4) The Inspector General shall have authority to administer to or take from any person an oath, affirmation, or affidavit, whenever necessary in the performance of his duties, which oath, affirmation, or affidavit when administered or taken by or before an employee of the Office designated by the Inspector General shall have the same force and effect as if administered or taken by or before an officer having a seal.

(5)(A) Except as provided in subparagraph (B), the Inspector General is authorized to require by subpoena the production of all information, documents, reports, answers, records, accounts, papers, and other data in any medium (including electronically stored information or any tangible thing) and documentary evidence necessary in the performance of the duties and responsibilities of the Inspector General.

(B) In the case of Government agencies, the Inspector General shall obtain information, documents, reports, answers, records, accounts, papers, and other data and evidence for the purpose specified in subparagraph (A) using procedures other than by subpoenas.

(C) The Inspector General may not issue a subpoena for or on behalf of any other element or component of the Agency.

(D) In the case of contumacy or refusal to obey a subpoena issued under this paragraph, the subpoena shall be enforceable by order of any appropriate district court of the United States.

(6) The Inspector General shall be provided with appropriate and adequate office space at central and field office locations, together with such equipment, office supplies, maintenance services, and communications facilities and services as may be necessary for the operation of such offices.

(7)(A) Subject to applicable law and the policies of the Director, the Inspector General shall select, appoint and employ such officers and employees as may be necessary to carry out his functions. In making such selections, the Inspector General shall ensure that such officers and employees have the requisite training and experience to enable him to carry out his duties effectively. In this regard, the Inspector General shall create within his organization a career cadre of sufficient size to provide appropriate continuity and objectivity needed for the effective performance of his duties.

(B) Consistent with budgetary and personnel resources allocated by the Director, the Inspector General has final approval of—

- (i) the selection of internal and external candidates for employment with the Office of Inspector General; and
- (ii) all other personnel decisions concerning personnel permanently assigned to the Office of Inspector General, including selection and appointment to the Senior Intelligence Service, but excluding all security-based determinations that are not within the authority of a head of other Central Intelligence Agency offices.

(C)(i) The Inspector General may designate an officer or employee appointed in accordance with subparagraph (A) as a law enforcement officer solely for purposes of subchapter III of chapter 83 or chapter 84 of title 5, United States Code, if such officer or employee is appointed to a position with responsibility for investigating suspected offenses against the criminal laws of the United States.

(ii) In carrying out clause (i), the Inspector General shall ensure that any authority under such clause is exercised in a manner consistent with section 3307 of title 5, United States Code, as it relates to law enforcement officers.

(iii) For purposes of applying sections 3307(d), 8335(b), and 8425(b) of title 5, United States Code, the Inspector General may exercise the functions, powers, and duties of an agency head or appointing authority with respect to the Office.

(8)(A) The Inspector General shall—

(i) appoint a Counsel to the Inspector General who shall report to the Inspector General; or

(ii) obtain the services of a counsel appointed by and directly reporting to another Inspector General or the Council of the Inspectors General on Integrity and Efficiency on a reimbursable basis.

(B) The counsel appointed or obtained under subparagraph (A) shall perform such functions as the Inspector General may prescribe.

(9)(A) The Inspector General may request such information or assistance as may be necessary for carrying out the duties and responsibilities of the Inspector General provided by this section from any Federal, State, or local governmental agency or unit thereof.

(B) Upon request of the Inspector General for information or assistance from a department or agency of the Federal Government, the head of the department or agency involved, insofar as practicable and not in contravention of any existing statutory restriction or regulation of such department or agency, shall furnish to the Inspector General, or to an authorized designee, such information or assistance.

(C) Nothing in this paragraph may be construed to provide any new authority to the Central Intelligence Agency to conduct intelligence activity in the United States.

(D) In this paragraph, the term “State” means each of the several States, the District of Columbia, the Commonwealth of Puerto Rico, the Commonwealth of the Northern Mariana Islands, and any territory or possession of the United States.

(f) SEPARATE BUDGET ACCOUNT.—

(1) Beginning with fiscal year 1991, and in accordance with procedures to be issued by the Director of National Intelligence in consultation with the intelligence committees, the Director of National Intelligence shall

include in the National Intelligence Program budget a separate account for the Office of Inspector General established pursuant to this section.

(2) For each fiscal year, the Inspector General shall transmit a budget estimate and request through the Director to the Director of National Intelligence that specifies for such fiscal year

(A) the aggregate amount requested for the operations of the Inspector General;

(B) the amount requested for all training requirements of the Inspector General, including a certification from the Inspector General that the amount requested is sufficient to fund all training requirements for the Office; and

(C) the amount requested to support the Council of the Inspectors General on Integrity and Efficiency, including a justification for such amount.

(3) In transmitting a proposed budget to the President for a fiscal year, the Director of National Intelligence shall include for such fiscal year

(A) the aggregate amount requested for the Inspector General of the Central Intelligence Agency;

(B) the amount requested for Inspector General training;

(C) the amount requested to support the Council of the Inspectors General on Integrity and Efficiency; and

(D) the comments of the Inspector General, if any, with respect to such proposed budget.

(4) The Director of National Intelligence shall submit to the Committee on Appropriations and the Select Committee on Intelligence of the Senate and the Committee on Appropriations and the Permanent Select Committee on Intelligence of the House of Representatives for each fiscal year—

(A) a separate statement of the budget estimate transmitted pursuant to paragraph (2);

(B) the amount requested by the Director of National Intelligence for the Inspector General pursuant to paragraph (3)(A);

(C) the amount requested by the Director of National Intelligence for training of personnel of the Office of the Inspector General pursuant to paragraph (3)(B);

(D) the amount requested by the Director of National Intelligence for support for the Council of the Inspectors General on Integrity and Efficiency pursuant to paragraph (3)(C); and

(E) the comments of the Inspector General under paragraph (3)(D), if any, on the amounts requested pursuant to paragraph

(3), including whether such amounts would substantially inhibit the Inspector General from performing the duties of the Office.

(g) TRANSFER.—There shall be transferred to the Office the office of the Agency referred to as the “Office of Inspector General.” The personnel, assets, liabilities, contracts, property, records, and unexpended balances of appropriations, authorizations, allocations, and other funds employed, held, used, arising from, or available to such “Office of Inspector General” are hereby transferred to the Office established pursuant to this section.

(h) INFORMATION ON WEBSITE.—

(1) The Director of the Central Intelligence Agency shall establish and maintain on the homepage of the Agency’s publicly accessible website information relating to the Office of the Inspector General including methods to contact the Inspector General.

(2) The information referred to in paragraph (1) shall be obvious and facilitate accessibility to the information related to the Office of the Inspector General.

[INSPECTOR GENERAL FOR AGENCY CONTINUED]

[SEC. 17. 50 U.S.C. § 3517 note]

RULE OF CONSTRUCTION.—Subparagraph (C) of section 17(e)(7) of the Central Intelligence Agency Act of 1949 (50 U.S.C. 3517(e)(7)) [as added by P.L. 115-31] may not be construed to confer on the Inspector General of the Central Intelligence Agency, or any other officer or employee of the Agency, any police or law enforcement or internal security functions or authorities.

SPECIAL ANNUITY COMPUTATION RULES FOR CERTAIN EMPLOYEES’ SERVICE ABROAD

SEC. 18. [50 U.S.C. § 3518]

(a) Notwithstanding any provision of chapter 83 of title 5, United States Code, the annuity under subchapter III of such chapter of an officer or employee of the Central Intelligence Agency who retires on or after October 1, 1989, is not designated under section 203 of the Central Intelligence Agency Retirement Act, and has served abroad as an officer or employee of the Agency on or after January 1, 1987, shall be computed as provided in subsection (b).

(b)(1) The portion of the annuity relating to such service abroad that is actually performed at any time during the officer’s or employee’s first ten years of total service shall be computed at the rate and using the percent of average pay specified in section 8339(a)(3) of title 5, United States Code that is normally applicable only to so much of an employee’s total service as exceeds ten years.

(2) The portion of the annuity relating to service abroad as described in subsection (a) but that is actually performed at any time after the officer's or employee's first ten years of total service shall be computed as provided in section 8339(a)(3) of title 5, United States Code; but, in addition, the officer or employee shall be deemed for annuity computation purposes to have actually performed an equivalent period of service abroad during his or her first ten years of total service, and in calculating the portion of the officer's or employee's annuity for his or her first ten years of total service, the computation rate and percent of average pay specified in paragraph (1) shall also be applied to the period of such deemed or equivalent service abroad.

(3) The portion of the annuity relating to other service by an officer or employee as described in subsection (a) shall be computed as provided in the provisions of section 8339(a) of title 5, United States Code that would otherwise be applicable to such service.

(4) For purposes of this subsection, the term "total service" has the meaning given such term under chapter 83 of title 5, United States Code.

(c) For purposes of subsections (f) through (m) of section 8339 of title 5, United States Code, an annuity computed under this section shall be deemed to be an annuity computed under subsections (a) and (o) of section 8339 of title 5, United States Code.

(d) The provisions of subsection (a) of this section shall not apply to an officer or employee of the Central Intelligence Agency who would otherwise be entitled to a greater annuity computed under an otherwise applicable subsection of section 8339 of title 5, United States Code.

SPECIAL RULES FOR DISABILITY RETIREMENT AND DEATH-IN-SERVICE BENEFITS WITH RESPECT TO CERTAIN EMPLOYEES

SEC. 19. [50 U.S.C. § 3519]

(a) OFFICERS AND EMPLOYEES TO WHOM CIARDS SECTION 231 RULES APPLY.—Notwithstanding any other provision of law, an officer or employee of the Central Intelligence Agency subject to retirement system coverage under subchapter III of chapter 83 of title 5, United States Code who—

- (1) has five years of civilian service credit toward retirement under such subchapter III of chapter 83, title 5, United States Code;
- (2) has not been designated under section 203 of the Central Intelligence Agency Retirement Act (50 U.S.C. 403 note) as a participant in the Central Intelligence Agency Retirement and Disability System;
- (3) has become disabled during a period of assignment to the performance of duties that are qualifying toward such designation under such section 203; and

(4) satisfies the requirements for disability retirement under section 8337 of title 5, United States Code—

shall, upon his own application or upon order of the Director, be retired on an annuity computed in accordance with the rules prescribed in section 231 of such Act, in lieu of an annuity computed as provided by section 8337 of title 5, United States Code.

(b) SURVIVORS OF OFFICERS AND EMPLOYEES TO WHOM CIARDS SECTION 232 RULES APPLY.—Notwithstanding any other provision of law, in the case of an officer or employee of the Central Intelligence Agency subject to retirement system coverage under subchapter III of chapter 83, title 5, United States Code, who—

(1) has at least eighteen months of civilian service credit toward retirement under such subchapter III of chapter 83, title 5, United States Code;

(2) has not been designated under section 203 of the Central Intelligence Agency Retirement Act (50 U.S.C. 2013), as a participant in the Central Intelligence Agency Retirement and Disability System;

(3) prior to separation or retirement from the Agency, dies during a period of assignment to the performance of duties that are qualifying toward such designation under such section 203; and

(4) is survived by a surviving spouse, former spouse, or child as defined in section 102 of the Central Intelligence Agency Retirement Act³, who would otherwise be entitled to an annuity under section 8341 of title 5, United States Code—

such surviving spouse, former spouse, or child of such officer or employee shall be entitled to an annuity computed in accordance with section 232 of such Act, in lieu of an annuity computed in accordance with section 8341 of title 5, United States Code.

(c) ANNUITIES UNDER THIS SECTION DEEMED ANNUITIES UNDER CSRS.—The annuities provided under subsections (a) and (b) of this section shall be deemed to be annuities under chapter 83 of title 5, United States Code, for purposes of the other provisions of such chapter and other laws (including the Internal Revenue Code of 1986) relating to such annuities, and shall be payable from the Central Intelligence Agency Retirement and Disability Fund maintained pursuant to section 202 of the Central Intelligence Agency Retirement Act.

³ Language includes the U.S.C. execution of Pub. L. 102–496, §803(a)(3)(B)(iii) to reflect the probable intent of Congress.

**SPECIAL RULES FOR CERTAIN INDIVIDUALS INJURED BY REASON OF WAR,
INSURGENCY, HOSTILE ACT, TERRORIST ACTIVITIES, OR INCIDENTS
DESIGNATED BY THE DIRECTOR**

Sec. 19A. [50 U.S.C. § [3519b]]

(a) DEFINITIONS.—In this section:

(1) COVERED DEPENDENT.—The term “covered dependent” means a family member (as defined by the Director) of a covered employee who, on or after September 11, 2001—

(A) accompanies the covered employee to an assigned duty station in a foreign country; and

(B) becomes injured by reason of a qualifying injury.

(2) COVERED EMPLOYEE.—The term “covered employee” means an officer or employee of the Central Intelligence Agency who, on or after September 11, 2001 becomes injured by reason of a qualifying injury.

(3) COVERED INDIVIDUAL.—The term “covered individual” means an individual who—

(A)(i) is detailed to the Central Intelligence Agency from other agencies of the United States Government or from the Armed Forces; or

(ii) is affiliated with the Central Intelligence Agency, as determined by the Director; and

(B) who, on or after September 11, 2001, becomes injured by reason of a qualifying injury.

(3) QUALIFYING INJURY.—The term “qualifying injury” means the following:

(A) With respect to a covered dependent, an injury incurred—

(i) during a period in which the covered dependent is accompanying the covered employee to an assigned duty station in a foreign country;

(ii) in connection with war, insurgency, hostile act, terrorist activity, or an incident designated for purposes of this section by the Director; and

(iii) that was not the result of the willful misconduct of the covered dependent.

(B) With respect to a covered employee or a covered individual—

(i) an injury incurred—

(I) during a period of assignment to a duty station in a foreign country;

(II) in connection with war, insurgency, hostile act, or terrorist activity; and

(III) that was not the result of the willful misconduct of the covered employee or the covered individual; or

(ii) an injury incurred—

(I) in connection with an incident designated for purposes of this section by the Director; and

(II) that was not the result of the willful misconduct of the covered employee or the covered individual.

(b) ADJUSTMENT OF COMPENSATION FOR TOTAL DISABILITY RESULTING FROM CERTAIN INJURIES.—

(1) INCREASE.—The Director may increase the amount of monthly compensation paid to a covered employee under section 8105 of title 5, United States Code. Subject to paragraph (2), the Director may determine the amount of each such increase by taking into account—

(A) the severity of the qualifying injury;

(B) the circumstances by which the covered employee became injured; and

(C) the seniority of the covered employee.

(2) MAXIMUM.—Notwithstanding chapter 81 of title 5, United States Code, the total amount of monthly compensation increased under paragraph (1) may not exceed the monthly pay of the maximum rate of basic pay for GS-15 of the General Schedule under section 5332 of such title.

(c) COSTS FOR TREATING QUALIFYING INJURIES.—The Director may pay the costs of treating a qualifying injury of a covered employee, a covered individual, or a covered dependent, or may reimburse a covered employee, a covered individual, or a covered dependent for such costs, that are not otherwise covered by chapter 81 of title 5, United State Code, or other provision of Federal law.

(d) AUTHORITY TO MAKE PAYMENTS FOR QUALIFYING INJURIES TO THE BRAIN.

(1) DEFINITIONS — In this subsection:

(A) Covered dependent. The term “covered dependent” has the meaning given such term in subsection (a), except that the assigned duty station need not be in a foreign country.

(B) Qualifying injury. The term “qualifying injury” has the meaning given such term in subsection (a), except that the assigned duty station need not be in a foreign country.

(2) AUTHORITY—Notwithstanding any other provision of law but subject to paragraph (3), the Director may provide payment to a covered dependent, a covered employee, and a covered individual for a qualifying injury to the brain.

(3) FUNDING.—

(A) IN GENERAL.—Payment under paragraph (2) in a fiscal year may be made using any funds—

(i) appropriated specifically for payments under such paragraph; or

(ii) reprogrammed in accordance with section 504 of the National Security Act of 1947 (50 U.S.C. 3094).

(B) BUDGET.—For each fiscal year, the Director shall include with the budget justification materials submitted to Congress in support of the budget of the President for that fiscal year pursuant to section 1105(a) of title 31, United States Code, an estimate of the funds required in that fiscal year to make payments under paragraph (2).

(4) REGULATIONS—

(A) In general—The Director shall prescribe regulations to carry out this subsection.

(B) Elements—The regulations prescribed under subparagraph (A) shall include regulations detailing fair and equitable criteria for payment under paragraph (2).

(5) NO EFFECT ON OTHER BENEFITS—

(A) IN GENERAL.—Payments made under paragraph (2) are supplemental to any other benefit furnished by the United States Government for which a covered dependent, covered employee, or covered individual is entitled, and the receipt of such payments may not affect the eligibility of such a person to any other benefit furnished by the United States Government.

(B) RELATION TO CERTAIN FEDERAL WORKERS COMPENSATION LAWS.—Without regard to the requirements in sections (b) and (c), covered employees need not first seek benefits provided under chapter 81 of title 5, United States Code, to be eligible solely for payment authorized under paragraph (2) of this subsection.

GENERAL COUNSEL OF THE CENTRAL INTELLIGENCE AGENCY

SEC. 20. [50 U.S.C. § 3520]

(a) There is a General Counsel of the Central Intelligence Agency, appointed from civilian life by the President, by and with the advice and consent of the Senate.

(b) The General Counsel is the chief legal officer of the Central Intelligence Agency.

(c) The General Counsel of the Central Intelligence Agency shall perform such functions as the Director may prescribe.

CENTRAL SERVICES PROGRAM

SEC. 21. [50 U.S.C. § 3521]

(a) **IN GENERAL.**—The Director may carry out a program under which elements of the Agency provide items and services on a reimbursable basis to other elements of the Agency, nonappropriated fund entities or instrumentalities associated or affiliated with the Agency, and other Government agencies. The Director shall carry out the program in accordance with the provisions of this section.

(b) **PARTICIPATION OF AGENCY ELEMENTS.**—

(1) In order to carry out the program, the Director shall—

(A) designate the elements of the Agency that are to provide items or services under the program (in this section referred to as “central service providers”);

(B) specify the items or services to be provided under the program by such providers; and

(C) assign to such providers for purposes of the program such inventories, equipment, and other assets (including equipment on order) as the Director determines necessary to permit such providers to provide items or services under the program; and

(D) authorize such providers to make known their services to the entities specified in subsection (a) through Government communication channels.

(2) The designation of elements and the specification of items and services under paragraph (1) shall be subject to the approval of the Director of the Office of Management and Budget.

(3) The authority in paragraph (1)(D) does not include the authority to distribute gifts or promotional items.

(c) **CENTRAL SERVICES WORKING CAPITAL FUND.**—

(1) There is established a fund to be known as the Central Services Working Capital Fund (in this section referred to as the “Fund”). The purpose of the Fund is to provide sums for activities under the program.

(2) There shall be deposited in the Fund the following:

(A) Amounts appropriated to the Fund.

(B) Amounts credited to the Fund from payments received by central service providers under subsection (e).

(C) Fees imposed and collected under subsection (f)(1).

(D) Amounts received in payment for loss or damage to equipment or property of a central service provider as a result of activities under the program.

(E) Other receipts from the sale or exchange of equipment, recyclable materials, or property of a central service provider as a result of activities under the program.

(F) Receipts from individuals in reimbursement for utility services and meals provided under the program.

(G) Receipts from individuals for the rental of property and equipment under the program.

(H) Such other amounts as the Director is authorized to deposit in or transfer to the Fund.

(3) Amounts in the Fund shall be available, without fiscal year limitation, for the following purposes:

(A) To pay the costs of providing items or services under the program.

(B) To pay the costs of carrying out activities under subsections (b)(1)(D) and (f)(2).

(d) LIMITATION ON AMOUNT OF ORDERS.—The total value of all orders for items or services to be provided under the program in any fiscal year may not exceed an amount specified in advance by the Director of the Office of Management and Budget.

(e) PAYMENT FOR ITEMS AND SERVICES.—

(1) A Government agency provided items or services under the program shall pay the central service provider concerned for such items or services an amount equal to the costs incurred by the provider in providing such items or services plus any fee imposed under subsection (f). In calculating such costs, the Director shall take into account personnel costs (including costs associated with salaries, annual leave, and workers' compensation), plant and equipment costs (including depreciation of plant and equipment other than structures owned by the Agency), operation and maintenance expenses, amortized costs, and other expenses.

(2) Payment for items or services under paragraph (1) may take the form of an advanced payment by an agency from appropriations available to such agency for the procurement of such items or services.

(f) FEES.—

(1) The Director may permit a central service provider to impose and collect a fee with respect to the provision of an item or service under the program. The amount of the fee may not exceed an amount equal to four percent of the payment received by the provider for the item or service.

(2) The Director may obligate and expend amounts in the Fund that are attributable to the fees imposed and collected under paragraph (1) to acquire equipment or systems for, or to improve the equipment or systems of, central service providers and any elements of the Agency that are not designated for participation in the program in order to facilitate the designation of such elements for future participation in the program.

(g) TERMINATION.—

(1) Subject to paragraph (2), the Director of the Central Intelligence Agency and the Director of the Office of Management and Budget, acting jointly—

(A) may terminate the program under this section and the Fund at any time; and

(B) upon such termination, shall provide for the disposition of the personnel, assets, liabilities, grants, contracts, property, records, and unexpended balances of appropriations, authorizations, allocations, and other funds held, used, arising from, available to, or to be made available in connection with the program or the Fund.

(2) The Director of the Central Intelligence Agency and the Director of the Office of Management and Budget may not undertake any action under paragraph (1) until 60 days after the date on which the Directors jointly submit notice of such action to the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate.

DETAIL OF EMPLOYEES

SEC. 22. [50 U.S.C. § 3522]

The Director may—

(1) detail any personnel of the Agency on a reimbursable basis indefinitely to the National Reconnaissance Office without regard to any limitation under law on the duration of details of Federal Government personnel; and

(2) hire personnel for the purpose of any detail under paragraph (1).

INTELLIGENCE OPERATIONS AND COVER ENHANCEMENT AUTHORITY

Sec. 23. [50 U.S.C. § 3523]

(a) DEFINITIONS.—In this section—

(1) the term “designated employee” means an employee designated by the Director of the Central Intelligence Agency under subsection (b); and

(2) the term “Federal retirement system” includes the Central Intelligence Agency Retirement and Disability System, and the Federal Employees’ Retirement System (including the Thrift Savings Plan).

(b) IN GENERAL.—

(1) AUTHORITY.—Notwithstanding any other provision of law, the Director of the Central Intelligence Agency may exercise the authorities under this section in order to—

(A) protect from unauthorized disclosure—

- (i) intelligence operations;
- (ii) the identities of undercover intelligence officers;
- (iii) intelligence sources and methods; or
- (iv) intelligence cover mechanisms; or

(B) meet the special requirements of work related to collection of foreign intelligence or other authorized activities of the Agency.

(2) DESIGNATION OF EMPLOYEES.—The Director of the Central Intelligence Agency may designate any employee of the Agency who is under nonofficial cover to be an employee to whom this section applies. Such designation may be made with respect to any or all authorities exercised under this section.

(c) COMPENSATION.—The Director of the Central Intelligence Agency may pay a designated employee salary, allowances, and other benefits in an amount and in a manner consistent with the nonofficial cover of that employee, without regard to any limitation that is otherwise applicable to a Federal employee. A designated employee may accept, utilize, and, to the extent authorized by regulations prescribed under subsection (i), retain any salary, allowances, and other benefits provided under this section.

(d) RETIREMENT BENEFITS.—

(1) IN GENERAL.—The Director of the Central Intelligence Agency may establish and administer a nonofficial cover employee retirement system for designated employees (and the spouse, former spouses, and survivors of such designated employees). A designated employee may not participate in the retirement system established under this paragraph and another Federal retirement system at the same time.

(2) CONVERSION TO OTHER FEDERAL RETIREMENT SYSTEM.—

(A) IN GENERAL.—A designated employee participating in the retirement system established under paragraph (1) may convert to coverage under the Federal retirement system which would otherwise apply to that employee at any appropriate time determined by the Director of the Central Intelligence Agency (including at the time of separation of service by reason of

retirement), if the Director of the Central Intelligence Agency determines that the employee's participation in the retirement system established under this subsection is no longer necessary to protect from unauthorized disclosure—

- (i) intelligence operations;
- (ii) the identities of undercover intelligence officers;
- (iii) intelligence sources and methods; or
- (iv) intelligence cover mechanisms.

(B) CONVERSION TREATMENT.—Upon a conversion under this paragraph—

- (i) all periods of service under the retirement system established under this subsection shall be deemed periods of creditable service under the applicable Federal retirement system;
- (ii) the Director of the Central Intelligence Agency shall transmit an amount for deposit in any applicable fund of that Federal retirement system that—

(I) is necessary to cover all employee and agency contributions including—

- (aa) interest as determined by the head of the agency administering the Federal retirement system into which the employee is converting; or
- (bb) in the case of an employee converting into the Federal Employees' Retirement System, interest as determined under section 8334(e) of title 5, United States Code; and

(II) ensures that such conversion does not result in any unfunded liability to that fund; and

- (iii) in the case of a designated employee who participated in an employee investment retirement system established under paragraph (1) and is converted to coverage under subchapter III of chapter 84 of title 5, United States Code, the Director of the Central Intelligence Agency may transmit any or all amounts of that designated employee in that employee investment retirement system (or similar part of that retirement system) to the Thrift Savings Fund.

(C) TRANSMITTED AMOUNTS.—

(i) IN GENERAL.—Amounts described under subparagraph (B)(ii) shall be paid from the fund or appropriation used to pay the designated employee.

(ii) OFFSET.—The Director of the Central Intelligence Agency may use amounts contributed by the designated employee to a retirement system established under paragraph (1) to offset amounts paid under clause (i).

(D) RECORDS.—The Director of the Central Intelligence Agency shall transmit all necessary records relating to a designated employee who converts to a Federal retirement system under this paragraph (including records relating to periods of service which are deemed to be periods of creditable service under subparagraph (B)) to the head of the agency administering that Federal retirement system.

(e) HEALTH INSURANCE BENEFITS.—

(1) IN GENERAL.—The Director of the Central Intelligence Agency may establish and administer a nonofficial cover employee health insurance program for designated employees (and the family of such designated employees). A designated employee may not participate in the health insurance program established under this paragraph and the program under chapter 89 of title 5, United States Code, at the same time.

(2) CONVERSION TO FEDERAL EMPLOYEES' HEALTH BENEFITS PROGRAM.—

(A) IN GENERAL.—A designated employee participating in the health insurance program established under paragraph (1) may convert to coverage under the program under chapter 89 of title 5, United States Code, at any appropriate time determined by the Director of the Central Intelligence Agency (including at the time of separation of service by reason of retirement), if the Director of the Central Intelligence Agency determines that the employee's participation in the health insurance program established under this subsection is no longer necessary to protect from unauthorized disclosure—

- (i) intelligence operations;
- (ii) the identities of undercover intelligence officers;
- (iii) intelligence sources and methods; or
- (iv) intelligence cover mechanisms.

(B) CONVERSION TREATMENT.—Upon a conversion under this paragraph—

- (i) the employee (and family, if applicable) shall be entitled to immediate enrollment and coverage under chapter 89 of title 5, United States Code;

- (ii) any requirement of prior enrollment in a health benefits plan under chapter 89 of that title for continuation of coverage purposes shall not apply;
- (iii) the employee shall be deemed to have had coverage under chapter 89 of that title from the first opportunity to enroll for purposes of continuing coverage as an annuitant; and
- (iv) the Director of the Central Intelligence Agency shall transmit an amount for deposit in the Employees' Health Benefits Fund that is necessary to cover any costs of such conversion.

(C) TRANSMITTED AMOUNTS.—Any amount described under subparagraph (B)(iv) shall be paid from the fund or appropriation used to pay the designated employee.

(f) LIFE INSURANCE BENEFITS.—

(1) IN GENERAL.—The Director of the Central Intelligence Agency may establish and administer a nonofficial cover employee life insurance program for designated employees (and the family of such designated employees). A designated employee may not participate in the life insurance program established under this paragraph and the program under chapter 87 of title 5, United States Code, at the same time.

(2) CONVERSION TO FEDERAL EMPLOYEES GROUP LIFE INSURANCE PROGRAM.—

(A) IN GENERAL.—A designated employee participating in the life insurance program established under paragraph (1) may convert to coverage under the program under chapter 87 of title 5, United States Code at any appropriate time determined by the Director of the Central Intelligence Agency (including at the time of separation of service by reason of retirement), if the Director of the Central Intelligence Agency determines that the employee's participation in the life insurance program established under this subsection is no longer necessary to protect from unauthorized disclosure—

- (i) intelligence operations;
- (ii) the identities of undercover intelligence officers;
- (iii) intelligence sources and methods; or
- (iv) intelligence cover mechanisms.

(B) CONVERSION TREATMENT.—Upon a conversion under this paragraph—

- (i) the employee (and family, if applicable) shall be entitled to immediate coverage under chapter 87 of title 5, United States Code;

- (ii) any requirement of prior enrollment in a life insurance program under chapter 87 of that title for continuation of coverage purposes shall not apply;
- (iii) the employee shall be deemed to have had coverage under chapter 87 of that title for the full period of service during which the employee would have been entitled to be insured for purposes of continuing coverage as an annuitant; and
- (iv) the Director of the Central Intelligence Agency shall transmit an amount for deposit in the Employees' Life Insurance Fund that is necessary to cover any costs of such conversion.

(C) TRANSMITTED AMOUNTS.—Any amount described under subparagraph (B)(iv) shall be paid from the fund or appropriation used to pay the designated employee.

(g) EXEMPTION FROM CERTAIN REQUIREMENTS.—The Director of the Central Intelligence Agency may exempt a designated employee from mandatory compliance with any Federal regulation, rule, standardized administrative policy, process, or procedure that the Director of the Central Intelligence Agency determines—

- (1) would be inconsistent with the nonofficial cover of that employee; and
- (2) could expose that employee to detection as a Federal employee.

(h) TAXATION AND SOCIAL SECURITY.—

(1) IN GENERAL.—Notwithstanding any other provision of law, a designated employee—

(A) shall file a Federal or State tax return as if that employee is not a Federal employee and may claim and receive the benefit of any exclusion, deduction, tax credit, or other tax treatment that would otherwise apply if that employee was not a Federal employee, if the Director of the Central Intelligence Agency determines that taking any action under this paragraph is necessary to—

- (i) protect from unauthorized disclosure—
 - (I) intelligence operations;
 - (II) the identities of undercover intelligence officers;
 - (III) intelligence sources and methods; or
 - (IV) intelligence cover mechanisms; and
- (ii) meet the special requirements of work related to collection of foreign intelligence or other authorized activities of the Agency; and

(B) shall receive social security benefits based on the social security contributions made.

(2) INTERNAL REVENUE SERVICE REVIEW.—The Director of the Central Intelligence Agency shall establish procedures to carry out this subsection. The procedures shall be subject to periodic review by the Internal Revenue Service.

(i) REGULATIONS.—The Director of the Central Intelligence Agency shall prescribe regulations to carry out this section. The regulations shall ensure that the combination of salary, allowances, and benefits that an employee designated under this section may retain does not significantly exceed, except to the extent determined by the Director of the Central Intelligence Agency to be necessary to exercise the authority in subsection (b), the combination of salary, allowances, and benefits otherwise received by Federal employees not designated under this section.

(j) FINALITY OF DECISIONS.—Any determinations authorized by this section to be made by the Director of the Central Intelligence Agency or the Director's designee shall be final and conclusive and shall not be subject to review by any court.

(k) SUBSEQUENTLY ENACTED LAWS.—No law enacted after the effective date of this section shall affect the authorities and provisions of this section unless such law specifically refers to this section.

OFFICE OF THE OMBUDSMAN FOR ANALYTIC OBJECTIVITY

SEC. 24. [50 U.S.C. § 3525]

(a) ESTABLISHMENT.—

(1) IN GENERAL.—There is established in the Agency an Office of the Ombudsman for Analytic Objectivity (in this section referred to as the “Office”).

(2) APPOINTMENT OF OMBUDSMAN.—The Office shall be headed by an Ombudsman, who shall be appointed by the Director from among current or former senior staff officers of the Agency.

(b) DUTIES AND RESPONSIBILITIES.—The Ombudsman shall—

(1) on an annual basis, conduct a survey of analytic objectivity among officers and employees of the Agency;

(2) implement a procedure by which any officer or employee of the Agency may submit to the Office a complaint alleging politicization, bias, lack of objectivity, or other issues relating to a failure of tradecraft in analysis conducted by the Agency;

(3) except as provided in paragraph (4), upon receiving a complaint submitted pursuant to paragraph (2), take reasonable action to investigate the complaint, make a determination as to whether the incident described

in the complaint involved politicization, bias, or lack of objectivity, and prepare a report that—

(A) summarizes the facts relevant to the complaint;

(B) documents the determination of the Ombudsman with respect to the complaint; and

(C) contains a recommendation for remedial action;

(4) if a complaint submitted pursuant to paragraph (2) alleges politicization, bias, or lack of objectivity in the collection of intelligence information, refer the complaint to the official responsible for supervising collection operations of the Agency; and

(5) continuously monitor changes in areas of analysis that the Ombudsman determines involve a heightened risk of politicization, bias, or lack of objectivity, to ensure that any change in the analytic line arises from proper application of analytic tradecraft and not as a result of politicization, bias, or lack of objectivity.

(c) **REPORTS.**—(1) On an annual basis, the Ombudsman shall submit to the intelligence committees a report on the results of the survey conducted pursuant to subsection (b)(1) with respect to the most recent fiscal year.

(2) On an annual basis, the Ombudsman shall submit to the intelligence committees a report that includes—

(A) the number of complaints of [sic] submitted pursuant to subsection (b)(2) during the most recent fiscal year; and

(B) a description of the nature of such complaints, the actions taken by the Office or any other relevant element or component of the Agency with respect to such complaints, and the resolution of such complaints.

(3) On a quarterly basis, the Ombudsman shall submit to the intelligence committees a report that includes—

(A) a list of the areas of analysis monitored during the most recent calendar quarter pursuant to subsection (b)(5); and

(B) a brief description of the methods by which the Office has conducted such monitoring.

(d) **INTELLIGENCE COMMITTEES DEFINED.**—In this section, the term ‘intelligence committees’ means the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate.

IMPROVEMENT OF EDUCATION IN SCIENCE, TECHNOLOGY, ENGINEERING, ARTS, AND MATHEMATICS

SEC. 25 [50 U.S.C. § 3526]

(a) **DEFINITIONS.**—In this section:

(1) ELIGIBLE ENTITY.—The term “eligible entity” includes a department or agency of the Federal Government, a State, a political subdivision of a State, an individual, and a not-for-profit or other organization in the private sector.

(2) EDUCATIONAL INSTITUTION.—The term “educational institution” includes any public or private elementary school or secondary school, institution of higher education, college, university, or any other profit or nonprofit institution that is dedicated to improving science, technology, engineering, the arts, mathematics, business, law, medicine, or other fields that promote development and education relating to science, technology, engineering, the arts, or mathematics.

(3) STATE.—The term “State” means each of the several States, the District of Columbia, the Commonwealth of Puerto Rico, the Commonwealth of the Northern Mariana Islands, and any other territory or possession of the United States.

(b) REQUIREMENTS.—The Director shall, on a continuing basis—

(1) identify actions that the Director may take to improve education in the scientific, technology, engineering, arts, and mathematics (known as “STEAM”) skills necessary to meet the long-term national security needs of the United States for personnel proficient in such skills; and

(2) establish and conduct programs to carry out such actions.

(c) AUTHORITIES.—

(1) IN GENERAL.—The Director, in support of educational programs in science, technology, engineering, the arts, and mathematics, may—

(A) award grants to eligible entities;

(B) provide cash awards and other items to eligible entities;

(C) accept voluntary services from eligible entities;

(D) support national competition judging, other educational event activities, and associated award ceremonies in connection with such educational programs; and

(E) enter into one or more education partnership agreements with educational institutions in the United States for the purpose of encouraging and enhancing study in science, technology, engineering, the arts, and mathematics disciplines at all levels of education.

(2) EDUCATION PARTNERSHIP AGREEMENTS.—

(A) NATURE OF ASSISTANCE PROVIDED.—Under an education partnership agreement entered into with an educational institution under paragraph (1)(E), the Director may provide assistance to the educational institution by—

- (i) loaning equipment to the educational institution for any purpose and duration in support of such agreement that the Director considers appropriate;
- (ii) making personnel available to teach science courses or to assist in the development of science courses and materials for the educational institution;
- (iii) providing sabbatical opportunities for faculty and internship opportunities for students;
- (iv) involving faculty and students of the educational institution in Agency projects, including research and technology transfer or transition projects;
- (v) cooperating with the educational institution in developing a program under which students may be given academic credit for work on Agency projects, including research and technology transfer for transition projects; and
- (vi) providing academic and career advice and assistance to students of the educational institution.

(B) **PRIORITIES.**—In entering into education partnership agreements under paragraph (1)(E), the Director shall prioritize entering into education partnership agreements with the following:

- (i) Historically Black colleges and universities and other minority-serving institutions, as described in section 371(a) of the Higher Education Act of 1965 (20 U.S.C. 1067q(a)).
- (ii) Educational institutions serving women, members of minority groups, and other groups of individuals who traditionally are involved in the science, technology, engineering, arts, and mathematics professions in disproportionately low numbers.

(d) **DESIGNATION OF ADVISOR.**—The Director shall designate one or more individuals within the Agency to advise and assist the Director regarding matters relating to science, technology, engineering, the arts, and mathematics education and training.

CHAPLAIN CORPS AND CHIEF OF CHAPLAINS

SEC. 26 [50 U.S.C. § 3527]

- (a) **ESTABLISHMENT OF CHAPLAIN CORPS.**— There is in the Agency a Chaplain Corps for the provision of spiritual or religious pastoral services.
- (b) **CHIEF OF CHAPLAINS.**—The head of the Chaplain Corps shall be the Chief of Chaplains, who shall be appointed by the Director.
- (c) **STAFF AND ADMINISTRATION.**—

- (1) STAFF.—The Director may appoint and fix the compensation of such staff of the Chaplain Corps as the Director considers appropriate, except that the Director may not—
- (A) appoint more than 10 full-time equivalent positions; or
 - (B) provide basic pay to any member of the staff of the Chaplain Corps at an annual rate of basic pay in excess of the maximum rate of basic pay for grade GS–15 as provided in section 5332 of title 5, United States Code.
- (2) ADMINISTRATION.—The Director may—
- (A) reimburse members of the staff of the Chaplain Corps for work-related travel expenses;
 - (B) provide security clearances to such members;
 - (C) furnish such physical workspace at the headquarters building of the Agency as the Director considers appropriate; and
 - (D) certify that all Chaplains meet common standards for professional chaplaincy and board certification by a national chaplaincy and pastoral care organization or equivalent.

COMPENSATION AND PROFESSIONAL STANDARD FOR CERTAIN MEDICAL OFFICERS

SEC. 27 [50 U.S.C. § 3528]

- (a) OFFICE OF MEDICAL SERVICES.— There is in the Agency an Office of Medical Services.
- (b) COMPENSATION.—Beginning not later than 1 year after the date of the enactment of the Intelligence Authorization Act for Fiscal Year 2022, each medical officer of the Office of Medical Services who meets the qualifications under subsection (c) shall be compensated during a pay period pursuant to a pay range that is equal to the pay range published in the Federal Register pursuant to section 7431(e)(1)(C) of title 38, United States Code (for the corresponding pay period), for a physician in the Veterans Health Administration in the District of Columbia region with a medical subspecialty that is the equivalent of the medical subspecialty of the officer.
- (c) CLINICAL PRACTICE QUALIFICATIONS.—A medical officer meets the qualifications under this subsection if the officer provides direct care services to patients in connection with the official duties of the officer and—
- (1) maintains current, active, full, and unrestricted licensure or registration as a physician from a State, the District of Columbia, or a commonwealth or territory of the United States;
 - (2) holds active board certification and maintains accreditation in an American Board of Medical Specialties direct care clinical specialty; and
 - (3) except as provided in subsection (d), maintains a minimum of 96

hours per year of clinical practice in an accredited clinic or hospital facility that is not affiliated with the Central Intelligence Agency.

(d) EXCEPTION FOR OVERSEAS SERVICE.—If a medical officer is a medical officer located in a duty station outside of the United States pursuant to a permanent change of station and greater than 50 percent of the official duties of the officer in such duty station involve direct patient care, the officer, in lieu of performing the minimum hours under subsection (c)(3) on an annual basis, may count up to 480 hours of clinical practice performed as specified in such subsection prior to such change of station, to fulfill in advance the requirement under such subsection for up to 3 years.

(e) CLINICAL PRACTICE HOURS. —The head of the Office of Medical Services shall make available to medical officers excused absence time to allow for the maintenance of clinical practice hours in accordance with subsection (c)(3).

MEDICAL ADVISORY BOARD.

SEC. 28 [50 U.S.C. § 3529]

(a) ESTABLISHMENT.— The Director shall establish within the Agency an office a medical advisory board (in this section referred to as the “Board”).

(b) DUTIES.—The Board shall-

(1) conduct a study on the Office of Medical Services of the Agency, and submit reports regarding such study, in accordance with subsection (c); and

(2) upon request, provide advice and guidance in connection with any independent review of the Office conducted by an inspector general.

(c) STUDY.—

(1) OBJECTIVES.—In conducting the study under subsection (b)(1), the Board shall seek to—

(A) contribute to the modernization and reform of the Office of Medical Services;

(B) ensure that the activities of the Office are of the highest professional quality; and

(C) ensure that all medical care provided by the Office is provided in accordance with the highest professional medical standards.

(2) REPORTS.—The Board shall submit to the congressional intelligence committees, in writing—

(A) interim reports on the study; and

(B) a final report on the study, which shall—

(i) set forth in detail the findings of the study and the recommendations of the Board, based on such findings and taking into consideration the objectives under paragraph (1),

regarding any changes to the activities of the Office of Medical Services; and

(ii) include, as applicable, any additional or dissenting views submitted by a member of the Board.

(d) MEMBERSHIP.—

(1) NUMBER AND APPOINTMENT.—The Board shall be composed of 9 members, appointed as follows:

(A) 1 member appointed by the Speaker of the House of Representatives.

(B) 1 member appointed by the minority leader of the House of Representatives.

(C) 1 member appointed by the majority leader of the Senate.

(D) 1 member appointed by the minority leader of the Senate.

(E) 1 member appointed by the Chairman of the Permanent Select Committee on Intelligence of the House of Representatives.

(F) 1 member appointed by the ranking minority member of the Permanent Select Committee on Intelligence of the House of Representatives.

(G) 1 member appointed by the Chairman of the Select Committee on Intelligence of the Senate.

(H) 1 member appointed by the Vice Chairman of the Select Committee on Intelligence of the Senate.

(I) 1 member appointed by the Director of National Intelligence.

(2) CHAIRPERSON.—During the first meeting under subsection (e)(1), the members of the Board shall elect a Chairperson of the Board. In addition to meeting the criteria under paragraph (3), the Chairperson may not be an employee, or former employee, of the Agency.

(3) CRITERIA.—The members appointed under paragraph (1) shall meet the following criteria:

(A) Each member shall be a recognized expert in at least 1 medical field, as demonstrated by appropriate credentials.

(B) Each member shall possess significant and diverse medical experience, including clinical experience.

(C) Each member shall be eligible to hold an appropriate security clearance.

(4) TERMS.—

(A) IN GENERAL.—Each member, including the Chairperson, shall be appointed or elected, as applicable, for the life of the Board.

(B) VACANCIES.—Any vacancy in the Board occurring prior to the expiration of the term under subparagraph (A) shall be filled in the manner in which the original appointment or election was made.

(5) COMPENSATION AND TRAVEL EXPENSES.—

(A) COMPENSATION.—Except as provided in subparagraph (B), each member of the Board, including the Chairperson, may be compensated at not to exceed the daily equivalent of the annual rate of basic pay in effect for a position at level IV of the Executive Schedule under section 5315 of title 5, United States Code, for each day during which that member is engaged in the actual performance of the duties under subsection (b).

(B) EXCEPTION FOR FEDERAL EMPLOYEES.—Members of the Board, including the Chairperson, who are officers or employees of the United States shall receive no additional pay by reason of the service of the member on the Board.

(C) TRAVEL EXPENSES.—Each member of the Board, including the Chairperson, while away from the home or regular places of business of the member in the performance of services for the Board, may be allowed travel expenses, including per diem in lieu of subsistence, in the same manner as persons employed intermittently in the Government service are allowed expenses under section 5703 of title 5, United States Code.

(6) DETAILEES.—

(A) IN GENERAL.—Upon request of the Board, the Director of National Intelligence may detail to the Board, without reimbursement from the Board, any of the personnel of the Office of the Director of National Intelligence to assist in carrying out the duties under subsection (b). Any such detailed personnel shall retain the rights, status, and privileges of the regular employment of the personnel without interruption.

(B) CLEARANCE.—Any personnel detailed to the Board under subparagraph (A) shall possess a security clearance in accordance with applicable laws and regulations concerning the handling of classified information.

(e) MEETINGS.—

(1) BOARD MEETINGS.—The Board shall meet not less frequently than on a quarterly basis.

(2) MEETINGS WITH CONGRESS.—The Board shall meet with the congressional intelligence committees on a biannual basis.

(f) INFORMATION ACCESS.—

(1) IN GENERAL.—Except as provided in paragraph (2), the Board may secure directly from any department or agency of the United States Government information necessary to enable it to carry out the duties under subsection (b) and, upon request of the Chairperson of the Board, the head of that department or agency shall furnish such information to the Board.

(2) EXCEPTION.—The Director (without delegation) may deny a request for information made by the Board pursuant to paragraph (1), regardless of the agency from which such information is requested.

(3) NOTIFICATION REQUIREMENT.—If the Director denies a request under paragraph (2), not later than 15 days after the date of such denial, the Director shall submit to the congressional intelligence committees a written notification of such denial.

(4) BRIEFINGS.—The Director shall ensure that the Board receives comprehensive briefings on all activities of the Office of Medical Services, including by promptly scheduling such briefings at the request of the Board.

(g) TERMINATION.—The Board shall terminate on the date that is 5 years after the date of the first meeting of the Board.

(h) DEFINITIONS.—In this section, the terms ‘congressional intelligence committees’ and ‘intelligence community’ have the meanings given such terms in section 3 of the National Security Act of 1947 (50 U.S.C. 3003).’

OFFICE OF WELLNESS AND WORKFORCE SUPPORT.

SEC. 29 [50 U.S.C. § 3530]

(a) ESTABLISHMENT.— The Director shall establish within the Agency an office (in this section referred to as the “Office”) to provide support for the physical health, mental health, and wellbeing of eligible individuals under subsection (d).

(b) Chief Wellbeing Officer; Assigned Staff.—

(1) Chief wellbeing officer.—The head of the Office is the Chief Wellbeing Officer, who shall provide to the Director regular updates on the operations of the Office.

(2) Assigned staff.—To assist in performing the functions under subsection (c), the Director shall assign to the Office a sufficient number of individuals, who shall have no official duties other than duties related to the Office while so assigned.

(c) Functions of Office.—

(1) Functions.—The Director shall establish the functions and role of the Office, which shall include the following:

(A) Providing to eligible individuals under subsection (d) advice and assistance on health and wellbeing, including with respect to—

- (i) physical health and access to physical health care;
- (ii) mental health and access to mental health care; and
- (iii) other related programs and benefits for which the individual may be eligible.

(B) In providing advice and assistance to individuals under subparagraph (A), assisting such individuals who are applying for,

and navigating the process to obtain, benefits furnished by the United States Government for which the individual is eligible, including, at a minimum—

- (i) health care and benefits described in such subparagraph; and
- (ii) benefits furnished pursuant to section 19A.

(C) Maintaining, and making available to eligible individuals under subsection (d), the following:

- (i) A list of physicians and mental health care providers (including from the private sector, as applicable), who have experience with the physical and mental health care needs of the Agency workforce.
- (ii) A list of chaplains and religious counselors who have experience with the needs of the Agency workforce, including information regarding access to the Chaplain Corps established under section 26.
- (iii) Information regarding how to select and retain private attorneys who have experience with the legal needs of the Agency workforce, including detailed information on the process for the appropriate sharing of information with retained private attorneys.

(D) Any other functions the Director determines appropriate.

(2) Rule of construction.—The inclusion of any person on a list maintained or made available pursuant to paragraph (1)(C) shall not be construed as an endorsement of such person (or any service furnished by such person), and the Director shall not be liable, as a result of such inclusion, for any portion of compensable injury, loss, or damage attributable to such person or service.

(3) Confidentiality.—

(A) Requirement.—The Director shall ensure that, to the extent permitted by law, the advice and assistance provided by the Office to eligible individuals under subsection (d) is provided in a confidential manner.

(B) Regulations.—The Director may prescribe regulations regarding the requirement for confidentiality under this paragraph. The Director shall submit to the congressional intelligence committees (as defined in section 3 of the National Security Act of 1947 (50 U.S.C. 3003)), the Subcommittee on Defense of the Committee on Appropriations of the Senate, and the Subcommittee on Defense of the Committee on Appropriations of the House of Representatives any such regulations not later than 30 days after prescribing such regulations.

(d) Eligibility.—

(1) In general.—An individual described in paragraph (2) may receive a service under the Office at the election of the individual.

(2) Individuals described.—An individual described in this paragraph is—

- (A) a current or former officer or employee of the Agency; or
- (B) an individual affiliated with the Agency, as determined by the Director.

SEXUAL ASSAULT AND SEXUAL HARASSMENT WITHIN THE AGENCY.

SEC. 30. [50 U.S.C. § 3531]

(a) RESPONSIBILITIES OF DIRECTOR.—The Director shall carry out the following responsibilities:

- (1) Establishing professional and uniform training for employees assigned to working with all aspects of the response of the Agency to allegations of sexual assault and sexual harassment.
- (2) Developing and implementing policies and procedures to protect the confidentiality of employees who report sexual assault or sexual harassment and to mitigate negative effects on the reputation or career of such an employee as a result of such a report.
- (3) Developing and implementing documented standards for—
 - (A) appropriate mitigation and protection measures for individuals who make allegations of a sexual assault or sexual harassment to be put in place while an investigation proceeds;
 - (B) appropriate employee consequences to be imposed based on the findings of an inquiry or investigation into a substantiated allegation of sexual assault or sexual harassment;
 - (C) appropriate career path protection for all employees involved in an incident resulting in a reported allegation of sexual assault or sexual harassment while an administrative or criminal investigation or review of the allegation is pending; and
 - (D) mitigation measures to protect employees and mission execution while such allegations are being addressed.
- (4) Articulating and enforcing norms, expectations, practices, and policies, including with respect to employee promotions and assignments, that are published for the workforce and designed to promote a healthy workplace culture that is inhospitable to sexual assault and sexual harassment.
- (5) Developing and issuing workforce messaging to inform Agency employees of policies, procedures, resources, and points of contact to

obtain information related to, or to report, sexual assault or sexual harassment globally.

(6) Developing and implementing sexual assault and sexual harassment training for all Agency employees that—

(A) is designed to strengthen individual knowledge, skills, and capacity to prevent and respond to sexual assault and sexual harassment;

(B) includes onboarding programs, annual refresher training, and specialized leadership training; and

(C) includes details of the definitions of sexual assault and sexual harassment, the distinction between such terms, and what does or does not constitute each.

(7) Developing and implementing processes and procedures applicable to personnel involved in providing the training referred to in paragraph (6) that—

(A) are designed to ensure seamless policy consistency and mechanisms for submitting reports of sexual assault and sexual harassment in all training environments; and

(B) include requirements for in-person training that—

(i) covers the reporting processes for sexual assault and sexual harassment that are specific to training environments for students and trainers; and

(ii) shall be provided at an appropriate time during the first 5 days of any extended or residential training course.

(8) Developing and implementing, in consultation with the Victim Advocacy Specialists of the Federal Bureau of Investigation, appropriate training requirements, policies, and procedures applicable to all employees whose professional responsibilities include interaction with people making reports alleging sexual assault or sexual harassment.

(9) Developing and implementing procedures under which current and former employees of the Agency who have reported an allegation of sexual assault or sexual harassment may obtain documents and records related to such a report, as appropriate and upon request.

(10) Developing and implementing procedures under which an employee who makes a restricted or unrestricted report containing an allegation of a sexual assault or sexual harassment may transfer out of the current assignment or location of the employee, upon the request of the employee making the report. Such procedures shall be consistent with the privilege established in section 31.

(11) Developing policies and procedures for the Special Victim Investigator, as applicable, to facilitate outside engagement requests of

employees reporting allegations of sexual assault or sexual harassment as described in sections 31 and 32.

(12) Coordinating the response of the Agency to allegations of sexual assault and sexual harassment.

(b) SEMIANNUAL REPORT.—Not less frequently than once every 180 days, the Director shall submit to the Select Committee on Intelligence of the Senate and the Permanent Select Committee on Intelligence of the House of Representatives a report on the activities of all Agency offices responsible for preventing, investigating, adjudicating, and addressing claims of sexual assault or sexual harassment. The Director shall personally review, approve, and submit each report under this subsection on a nondelegable basis. Each such report shall include—

(1) for the period covered by the report—

(A) the number of new allegations of sexual assault and sexual harassment reported to any Agency office, disaggregated by restricted and unrestricted reports;

(B) the number of new or ongoing cases in which the Sexual Harassment/Assault Response and Prevention Office has provided victim advocacy services;

(C) a description of all training activities related to sexual assault and sexual harassment carried out Agencywide, and the number of such trainings conducted; and

(2) for the period beginning on the date of the enactment of the Intelligence Authorization Act for Fiscal Year 2024 and ending on the last day of the period covered by the report—

(A) the total number of allegations of sexual assault and sexual harassment;

(B) the disposition of each report of such an allegation;

(C) any corrective action taken in response to each such report;

(D) the number of such allegations that were not substantiated; and

(E) the number of employee reassignment and relocation requests, including—

(i) the number of such requests that were granted;

(ii) the number of such requests that were denied; and

(iii) for any such request that was denied, the position of the individual who denied the request and the reason for denial.

(c) APPLICABILITY.—

(1) IN GENERAL.—The policies developed pursuant to this section shall apply to each of the following:

(A) Any employee of the Agency.

(B) Any person other than an Agency employee who alleges they were sexually assaulted or harassed at a facility associated with the

Agency or during the performance of a function associated with the Agency. If such person is an employee of an industrial contractor, the contracting officer for the relevant contract shall coordinate with the contractually identified representative for the prime contractor in a manner consistent with section 31.

(2) **RELATION TO EXISTING REGULATIONS.**—The policies developed pursuant to this section for handling allegations of sexual harassment shall be in addition to the requirements of part 1614 of title 29, Code of Federal Regulations, or successor regulations.

REPORTING AND INVESTIGATION OF ALLEGATIONS OF SEXUAL ASSAULT AND SEXUAL HARASSMENT.

SEC. 31 [50 U.S.C. § 3532]

(a) **POLICIES RELATING TO RESTRICTED AND UNRESTRICTED REPORTING OF SEXUAL ASSAULT AND SEXUAL HARASSMENT.**—

(1) **IN GENERAL.**—The Director shall develop and implement policies, regulations, personnel training, and workforce education to establish and provide information about restricted reports and unrestricted reports of allegations of sexual assault and sexual harassment within the Agency in accordance with this subsection.

(2) **WORKFORCE EDUCATION.**—Workforce education developed under paragraph (1) shall be designed to clearly inform Agency employees of the differences between restricted and unrestricted reporting of allegations of sexual assault and sexual harassment, and which individual or office within the Agency is responsible for receiving each type of report.

(3) **RELATIONSHIP TO THE SEXUAL HARASSMENT/ASSAULT RESPONSE AND PREVENTION OFFICE.**—To the extent consistent with preserving a victim's complete autonomy, the policies, regulations, training, and messaging described in this subsection shall—

(A) encourage Agency employees to make restricted or unrestricted reports of sexual assault and sexual harassment to the Sexual Harassment/Assault Response and Prevention Office;

(B) encourage Agency employees to use the Sexual Harassment/Assault Response and Prevention Office as the primary point of contact and entry point for Agency employees to make restricted or unrestricted reports of sexual assault and sexual harassment;

(C) encourage Agency employees to seek the victim advocacy services of the Sexual Harassment/Assault Response and Prevention Office after reporting an allegation of sexual assault or

sexual harassment, to the extent consistent with the victim's election; and

(D) encourage Agency employees and individuals who receive disclosures of sexual assault and sexual harassment to provide the report to, and receive guidance from, the Sexual Harassment/Assault Response and Prevention Office.

(b) ELECTION.—Any person making a report containing an allegation of a sexual assault or sexual harassment shall elect whether to make a restricted report or an unrestricted report. Once an election is made to make an unrestricted report, such election may not be changed.

(c) UNRESTRICTED REPORTS.—

(1) ASSISTANCE.—A person who elects to make an unrestricted report containing an allegation of sexual assault or sexual harassment may seek the assistance of another employee of the Agency with taking the action required under paragraph (2).

(2) ACTION REQUIRED.—A person electing to make an unrestricted report containing an allegation of sexual assault or sexual harassment shall submit the report to the Sexual Harassment/Assault Response and Prevention Office. To the extent consistent with the person's election after consultation with the Sexual Harassment/Assault Response and Prevention Office, the Sexual Harassment/Assault Response and Prevention Office may facilitate the person's contact with any other appropriate Agency official or office, and make available to Agency employees the following:

(A) A list of physicians and mental health care providers (including from the private sector, as applicable) who have experience with the physical and mental health care needs of the Agency workforce.

(B) A list of chaplains and religious counselors who have experience with the needs of the Agency workforce, including information regarding access to the Chaplain Corps established under section 26.

(C) Information regarding how to select and retain private attorneys who have experience with the legal needs of the Agency workforce, including detailed information on the process for the appropriate sharing of information with retained private attorneys.

(3) RULE OF CONSTRUCTION.—The inclusion of any person on a list maintained or made available pursuant to subsection (c)(2) shall not be construed as an endorsement of such person (or any service furnished by such person), and neither the Sexual Harassment/Assault Response and Prevention Office nor the Agency shall be liable, as a result of such

inclusion, for any portion of compensable injury, loss, or damage attributable to such person or service.

(d) RESTRICTED REPORTS.—

(1) PROCESS FOR MAKING REPORTS.—A person who elects to make a restricted report containing an allegation of sexual assault or sexual harassment shall submit the report to the Sexual Harassment/Assault Response and Prevention Office.

(2) ACTION REQUIRED.—A restricted report containing an allegation of sexual assault or sexual harassment—

(A) shall be treated by the person who receives the report in the same manner as a communication covered by the privilege set forth in this section;

(B) shall not result in a referral to law enforcement or commencement of a formal administrative investigation, unless the victim elects to change the report from a restricted report to an unrestricted report;

(C) in a case requiring an employee reassignment, relocation, or other mitigation or protective measures, shall result only in actions that are managed in a manner to limit, to the extent possible, the disclosure of any information contained in the report;

(D) shall be exempt from any Federal or, to the maximum extent permitted by the Constitution, State reporting requirements, including the requirements under section 535(b) of title 28, United States Code, section 17(b)(5) of this Act, relevant provisions of Executive Order 12333 (50 U.S.C. 3001 note; relating to United States intelligence activities), or successor order, Executive Order 13462 (50 U.S.C. 3001 note; relating to President's intelligence advisory board and intelligence oversight board), or successor order, title VII of the Civil Rights Act of 1964 (42 U.S.C. 2000e et seq.), the Age Discrimination in Employment Act of 1967 (29 U.S.C. 621 et seq.), title I of the Americans with Disabilities Act of 1990 (42 U.S.C. 12111 et seq.), and sections 501 and 505 of the Rehabilitation Act of 1973 (29 U.S.C. 791 and 794a), except when reporting is necessary to prevent or mitigate an imminent threat of serious bodily harm.

(3) RULE OF CONSTRUCTION.—The receipt of a restricted report submitted under subsection (d) shall not be construed as imputing actual or constructive knowledge of an alleged incident of sexual assault or sexual harassment to the Agency for the purpose of the Agency's responsibility to exercise reasonable care to take immediate and appropriate corrective action to prevent and correct harassing behavior.

(e) PRIVILEGED COMMUNICATIONS WITH AGENCY EMPLOYEES.—

(1) IN GENERAL.—A victim shall be entitled to maintain and assert a privilege against disclosure of, and be able to prevent any other person from disclosing, any confidential communication made between the victim and any employee of the Sexual Harassment/Assault Response and Prevention Office, if such communication was made for the purpose of facilitating advice or assistance to the victim in accordance with this section. A victim may consent to additional disclosures.

(2) WHEN A COMMUNICATION IS CONFIDENTIAL.—A communication is confidential for the purposes of this section if made in the course of the relationship between the victim and any employee of the Sexual Harassment/Assault Response and Prevention Office and not intended to be disclosed to third persons, other than those to whom disclosure is made in furtherance of the provision of advice or assistance to the victim or those reasonably necessary for such transmission of the communication.

(3) MAINTENANCE OF PRIVILEGE.—The privilege is maintained by the victim. A victim may authorize the Sexual Harassment/Assault Response and Prevention Office employee who received the communication to assert the privilege on his or her behalf, with confidentiality. The Sexual Harassment/Assault Response and Prevention Office employee who received the communication may assert the privilege on behalf of the victim. The authority of such Sexual Harassment/Assault Response and Prevention Office employee to so assert the privilege is presumed in the absence of evidence to the contrary.

(4) EXCEPTIONS.—The privilege shall not apply to prevent limited disclosures necessary under the following circumstances:

(A) When the victim is deceased.

(B) When the Sexual Harassment/Assault Response and Prevention Office employee who received the communication has a reasonable belief that a victim's mental or emotional condition makes the victim a danger to any person, including the victim.

(C) When the otherwise privileged communication clearly contemplates the future commission of a crime or breach of national security, or aiding any individual to commit or plan to commit what the victim knew or reasonable should have known to be a crime or breach of national security.

(D) When disclosure of a communication is constitutionally required.

(5) HANDLING OF EXCEPTIONS.—When the Sexual Harassment/Assault Response and Prevention Office employee determines that information requires an exception to the privilege, the Sexual Harassment/Assault Response and Prevention Office employee who received the

communication will protect information pertaining to the facts and circumstances surrounding the underlying sexual assault or sexual harassment allegations to the greatest extent possible.

(f) INCIDENT REPORTS WHEN VICTIM OR ALLEGED PERPETRATOR IS AN AGENCY EMPLOYEE.—

(1) INCIDENT REPORTING POLICY.—The Director shall establish and maintain a policy under which—

(A) the head of the Sexual Harassment/Assault Response and Prevention Office is required to submit a written incident report not later than 8 days after receiving an unrestricted report containing an allegation of sexual assault or sexual harassment; and

(B) each such incident report required under subparagraph (A) shall be provided to—

(i) the Director of the Agency;

(ii) the Chief Operating Officer of the Agency;

(iii) the Special Victim Investigator; and

(iv) such other individuals as the Director determines appropriate.

(2) PURPOSE.—The purpose of an incident report required under paragraph (1) is—

(A) to record the details about actions taken or in progress to provide the necessary care and support to the victim of the alleged incident;

(B) to document the referral of the allegations to the appropriate investigatory or law enforcement agency; and

(C) to provide initial formal notification of the alleged incident.

(3) ELEMENTS.—Each incident report required under paragraph (1) shall include each of the following:

(A) The time, date, and location of the alleged sexual assault or sexual harassment.

(B) An identification of the type of offense or harassment alleged.

(C) An identification of the assigned office and location of the victim.

(D) An identification of the assigned office and location of the alleged perpetrator, including information regarding whether the alleged perpetrator has been temporarily transferred or removed from an assignment or otherwise restricted, if applicable.

(E) A description of any post-incident actions taken in connection with the incident, including—

(i) referral to any services available to victims, including the date of each referral;

- (ii) notification of the incident to appropriate investigatory organizations, including the organizations notified and dates of notifications; and
- (iii) issuance of any personal protection orders or steps taken to separate the victim and the alleged perpetrator within their place of employment.

(F) Such other elements as the Director determines appropriate.

(g) COMMON PERPETRATOR NOTICE REQUIREMENT.—

(1) UNRESTRICTED REPORTS.—Upon receipt of an incident report under subsection (f)(1) containing an allegation of sexual assault or sexual harassment against an individual known to be the subject of at least one allegation of sexual assault or sexual harassment by another reporter, the Special Victim Investigator shall notify each of the following of all existing allegations against the individual:

- (A) The Director of the Agency.
- (B) The Chief Operating Officer of the Agency.
- (C) The Sexual Harassment/Assault Response and Prevention Office.

(D) If the individual is an Agency employee, the head of the directorate employing the individual and the firstlevel supervisor of the individual.

(E) If the individual is an Agency contractor, the Acquisition Group Chief and the contracting officer for the relevant contract. For industrial contractor personnel, the contracting officer shall notify the contractually identified representative for the prime contractor.

(F) The Inspector General of the Agency.

(G) Such other individuals as the Director determines appropriate.

(2) RESTRICTED REPORTS.—In the case of restricted reports under subsection (d), the Sexual Harassment/Assault Response and Prevention Office shall notify any victims known to have filed a restricted report against an individual known to be the subject of at least one unrestricted allegation of sexual assault or sexual harassment by another reporter that another allegation has been made against the same individual who is the alleged subject of the victim's report at the time of the victim's initial report or any time thereafter upon receipt of any subsequent unrestricted report under subsection (c) or a common perpetrator notice under paragraph (1) of this subsection.

(h) APPLICABILITY.—The policies developed pursuant to this section shall apply to each of the following:

- (1) Any employee of the Agency.

(2) Any person other than an Agency employee who alleges they were sexually assaulted or harassed at a facility associated with the Agency or during the performance of a function associated with the Agency.

(i) RECORDS.—

(1) IN GENERAL.—The Director shall establish a system for the tracking and, in accordance with chapter 31 of title 44, United States Code (commonly known as the ‘Federal Records Act of 1950’), long-term temporary retention of all Agency records related to any investigation into an allegation of sexual assault or sexual harassment made in an unrestricted report, including any related medical documentation.

(2) RELATION TO PRIVILEGE.—Any Agency records created under the authority of this section are subject to the privileges described in this section. Routine records management activities conducted by authorized Agency personnel with respect to such records, including maintaining, searching, or dispositioning of records, shall not result in a waiver of those privileges.

(3) APPLICABILITY TO FOIA.—This section shall constitute a withholding statute pursuant to section 552(b)(3) of title 5, United States Code, with respect to any information that may reveal the identity of a victim of sexual assault or sexual harassment, or any information subject to the privileges described in this section.

(j) RELATIONSHIP TO THE OFFICE OF EQUAL EMPLOYMENT OPPORTUNITY.—In the case of a restricted report of sexual harassment, such report shall not result in a referral to the Office of Equal Employment Opportunity, unless the victim elects to change the report from a restricted report to an unrestricted report. In the case of an unrestricted report, the Special Victim Investigator, the Office of Equal Employment Opportunity, law enforcement, or any other appropriate investigative body, or any appropriate combination thereof, may investigate the unrestricted report, as appropriate. Policies and procedures developed pursuant to this section are intended to offer victims options in addition to the process described in part 1614 of title 29, Code of Federal Regulations, or successor regulations.

(k) DEFINITIONS.—In this section:

(1) REPORT.—The term “report” means a communication—

(A) by a victim;

(B) that describes information relating to an allegation of sexual assault or sexual harassment;

(C) to an individual eligible to document an unrestricted or restricted report; and

(D) that the victim intends to result in formal documentation of an unrestricted or restricted report.

(2) VICTIM.—The term “victim” means a person who alleges they have suffered direct physical or emotional harm because they were subjected to sexual assault or sexual harassment.

SPECIAL VICTIM INVESTIGATOR.

SEC. 32. [50 U.S.C. § 3533]

(a) ESTABLISHMENT.—The Director shall establish in the Office of Security a Special Victim Investigator, who shall be authorized to investigate or facilitate the investigation of unrestricted reports containing allegations of sexual assault and sexual harassment. The person appointed as the Special Victim Investigator shall be an appropriately credentialed Federal law enforcement officer and may be detailed or assigned from a Federal law enforcement entity.

(b) RESPONSIBILITIES.—The Investigator shall—

- (1) at the election of a victim (as defined in section 31(k)), be authorized to conduct internal Agency inquiries, investigations, and other fact-finding activities related to allegations of sexual harassment, which may be separate and in addition to any inquiry or investigation conducted by the Office of Equal Employment Opportunity;
- (2) conduct and manage internal Agency inquiries, investigations, and other fact-finding activities related to specific allegations of sexual assault;
- (3) testify in a criminal prosecution in any venue, where appropriate;
- (4) serve as the case agent for a criminal investigation in any venue, where appropriate;
- (5) facilitate engagement with other law enforcement relating to such allegations, where appropriate, including coordinating on the matter and any related matters with other Federal, State, local, and Tribal law enforcement agencies, as necessary and appropriate, pursuant to regulations, requirements, and procedures developed in consultation with the Federal Bureau of Investigation, the Department of State’s Diplomatic Security Service, or other Federal, State, local, or Tribal law enforcement authorities, for any such inquiries, investigations, or other fact-finding activities;
- (6) develop and implement policies and procedures necessary for the Special Victim Investigator or any law enforcement partner to conduct effective investigations and also protect sensitive information;
- (7) serve as the primary internal investigative body in the Agency for allegations of sexual assault, except that, in the case of an allegation of a sexual assault involving an employee of the Office of Security, the Special Victim Investigator shall coordinate with the Inspector General or appropriate criminal investigators employed by a Federal, State, local,

or Tribal law enforcement entity, as necessary, to maintain the integrity of the investigation and mitigate potential conflicts of interest;

(8) establish and coordinate clear policies regarding which agency should take the lead on conducting, or be the lead in coordinating with local law enforcement when applicable, investigations of sexual assault and sexual harassment overseas; and

(9) sharing information with the Sexual Harassment/Assault Response and Prevention Office, including providing a copy of materials related to investigations with such redactions as deemed necessary, to facilitate the support and advocacy of such Office for victims of alleged sexual assault or sexual harassment.

- (c) **TIMEFRAME FOR INVESTIGATIONS.**—The Special Victim Investigator shall—
- (1) ensure that any Special Victim Investigator investigation into an allegation of a sexual assault or sexual harassment contained in an unrestricted report submitted under section 31 is completed by not later than 60 days after the date on which the report is referred to the Special Victim Investigator; and
- (2) if the Special Victim Investigator determines that the completion of an investigation will take longer than 60 days—
- (A) not later than 60 days after the date on which the report is referred to the Special Victim Investigator, submit to the Director a request for an extension that contains a summary of the progress of the investigation, the reasons why the completion of the investigation requires additional time, and a plan for the completion of the investigation; and
- (B) provide to the person who made the report and the person against whom the allegation in the report was made notice of the extension of the investigation.

SEPARATION PAY PROGRAM FOR VOLUNTARY SEPARATION FROM SERVICE

[50 U.S.C. § 3519a⁴]

- (a) **DEFINITIONS.**—For purposes of this section—
- (1) the term “Director” means the Director of the Central Intelligence Agency; and
- (2) the term “employee” means an employee of the Central Intelligence Agency, serving under an appointment without time limitation, who has been currently employed for a continuous period of at least 12 months, except that such term does not include—

⁴ This section was enacted as part of the Central Intelligence Agency Voluntary Separation Pay Act (P.L. 103-36), not the Central Intelligence Agency Act of 1949.

(A) a reemployed annuitant under subchapter III of chapter 83 or chapter 84 of title 5, United States Code, or another retirement system for employees of the Government; or

(B) an employee having a disability on the basis of which such employee is or would be eligible for disability retirement under any of the retirement systems referred to in subparagraph (A).

(b) ESTABLISHMENT OF PROGRAM.—In order to avoid or minimize the need for involuntary separations due to downsizing, reorganization, transfer of function, or other similar action, the Director may establish a program under which employees may be offered separation pay to separate from service voluntarily (whether by retirement or resignation). An employee who receives separation pay under such program may not be reemployed by the Central Intelligence Agency for the 12-month period beginning on the effective date of the employee's separation. An employee who receives separation pay under this section on the basis of a separation occurring on or after March 30, 1994, and accepts employment with the Government of the United States within 5 years after the date of the separation on which payment of the separation pay is based shall be required to repay the entire amount of the separation pay to the Central Intelligence Agency. If the employment is with an Executive agency (as defined by section 105 of title 5, United States Code), the Director of the Office of Personnel Management may, at the request of the head of the agency, waive the repayment if the individual involved possesses unique abilities and is the only qualified applicant available for the position. If the employment is with an entity in the legislative branch, the head of the entity or the appointing official may waive the repayment if the individual involved possesses unique abilities and is the only qualified applicant available for the position. If the employment is with the judicial branch, the Director of the Administrative Office of the United States Courts may waive the repayment if the individual involved possesses unique abilities and is the only qualified applicant available for the position.

(c) BAR ON CERTAIN EMPLOYMENT.—

(1) BAR.—An employee may not be separated from service under this section unless the employee agrees that the employee will not –

(A) act as agent or attorney for, or otherwise represent, any other person (except the United States) in any formal or informal appearance before, or, with the intent to influence, make any oral or written communication on behalf of any other person (except the United States) to the Central Intelligence Agency; or

(B) participate in any manner in the award, modification, extension, or performance of any contract for property or services with the Central Intelligence Agency, during the 12-month period beginning on the effective date of the employee's separation from service.

- (2) PENALTY.—An employee who violates an agreement under this subsection shall be liable to the United States in the amount of the separation pay paid to the employee pursuant to this section times the proportion of the 12-month period during which the employee was in violation of the agreement.
- (d) LIMITATIONS.—Under this program, separation pay may be offered only—
- (1) with the prior approval of the Director; and
 - (2) to employees within such occupational groups or geographic locations, or subject to such other similar limitations or conditions, as the Director may require.
- (e) AMOUNT AND TREATMENT FOR OTHER PURPOSES.—Such separation pay—
- (1) shall be paid in a lump sum;
 - (2) shall be equal to the lesser of—
 - (A) an amount equal to the amount the employee would be entitled to receive under section 5595(c) of title 5, United States Code, if the employee were entitled to payment under such section; or
 - (B) \$25,000;
 - (3) shall not be a basis for payment, and shall not be included in the computation, of any other type of Government benefit; and
 - (4) shall not be taken into account for the purpose of determining the amount of any severance pay to which an individual may be entitled under section 5595 of title 5, United States Code, based on any other separation.
- (f) REGULATIONS.—The Director shall prescribe such regulations as may be necessary to carry out this section.
- (g) REPORTING REQUIREMENTS.—
- (1) OFFERING NOTIFICATION.—The Director may not make an offering of voluntary separation pay pursuant to this section until 30 days after submitting to the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate a report describing the occupational groups or geographic locations, or other similar limitations or conditions, required by the Director under subsection (d).
 - (2) ANNUAL REPORT.—At the end of each of the fiscal years 1993 through 1997, the Director shall submit to the President and the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate a report on the effectiveness and costs of carrying out this section.

NATIONAL SECURITY AGENCY ACT OF 1959

[Public Law 86-36 of May 29, 1959; 73 STAT. 63]

AN ACT To provide certain administrative authorities for the National Security Agency, and for other purposes.

Be it enacted by the Senate and the House of Representatives of the United States of America in Congress assembled, That this Act may be cited as the “National Security Agency Act of 1959”.

TABLE OF CONTENTS¹

- SEC. 2. Director of the Agency and Director of Compliance.
- SEC. 3. [Amended Title 10.]
- SEC. 4. [Repealed.]
- SEC. 5. Additional compensation.
- SEC. 6. Disclosure of Agency’s organization, function, activities, or personnel.
- SEC. 7. [Repealed.]
- SEC. 8. Effective Date.
- SEC. 9. Support for activities and personnel outside the United States.
- SEC. 10. Language training and cryptologic linguist reserve programs.
- SEC. 11. Enhancement of security authorities.
- SEC. 12. Senior Cryptologic Executive Service.
- SEC. 13. Cryptologic research grant program.
- SEC. 14. Availability of appropriations.
- SEC. 15. Misuse of Agency name, initials, or seal.
- SEC. 16. Louis Stokes Educational Scholarship Program.
- SEC. 17. [Repealed.]
- SEC. 18. Transportation of remains of certain employees.
- SEC. 19. National Security Agency Emerging Technologies Panel.
- SEC. 20. Collection of service charges for certification or validation of information assurance products.
- SEC. 21. Senior Chief Petty Officer Shannon Kent Award for Distinguished Female Personnel.
- SEC. 22. Congressional notification by National Security Agency of intelligence collection adjustments.

¹ Table of Contents does not appear in the Act itself.

[DIRECTOR OF THE AGENCY AND DIRECTOR OF COMPLIANCE]

SEC. 2. [50 U.S.C. § 3602]

(a)(1) There is a Director of the National Security Agency.

(2) The Director of the National Security Agency shall be appointed by the President, by and with the advice and consent of the Senate.

(3) The Director of the National Security Agency shall be the head of the National Security Agency and shall discharge such functions and duties as are provided by this Act or otherwise by law or executive order.

(b) There is a Director of Compliance of the National Security Agency, who shall be appointed by the Director of the National Security Agency and who shall be responsible for the programs of compliance over mission activities of the National Security Agency.

[SEC. 3. Amended Title 10.]

[SEC. 4. Repealed.]

[ADDITIONAL COMPENSATION]

SEC. 5. [50 U.S.C. § 3604]

Officers and employees of the National Security Agency who are citizens or nationals of the United States may be granted additional compensation, in accordance with regulations which shall be prescribed by the Secretary of Defense, not in excess of additional compensation authorized by section 207 of the Independent Offices Appropriation Act, 1949, as amended (5 U.S.C. 118h) [see 5 U.S.C. § 5941], for employees whose rates of basic compensation are fixed by statute.

**[DISCLOSURE OF AGENCY'S ORGANIZATION,
FUNCTION, ACTIVITIES, OR PERSONNEL]**

SEC. 6. [50 U.S.C. § 3605]

(a) Except as provided in subsection (b) of this section, nothing in this Act or any other law (including, but not limited to, the first section and section 2 of the Act of August 28, 1935 (5 U.S.C. § 654) [repealed by Pub. L. 86-626] shall be construed to require the disclosure of the organization or any function of the National Security Agency, of any information with respect to the activities thereof, or of the names, titles, salaries, or number of the persons employed by such agency.

(b) The reporting requirements of section 1582 of title 10, United States Code, shall apply to positions established in the National Security Agency in the manner provided by section 4 of this Act.

[SEC. 7. Repealed.]

[EFFECTIVE DATE]

SEC. 8.

The foregoing provisions of this Act shall take effect on the first day of the first pay period which begins later than the thirtieth day following the date of enactment of this Act.

[SUPPORT FOR ACTIVITIES AND PERSONNEL OUTSIDE THE UNITED STATES]

SEC. 9. [50 U.S.C. § 3607]

(a) Notwithstanding section 322 of the Act of June 30, 1932 (40 U.S.C. 278a), section 5536 of title 5, United States Code, and section 2675 of title 10, United States Code, the Director of the National Security Agency, on behalf of the Secretary of Defense, may lease real property outside the United States, for periods not exceeding ten years, for the use of the National Security Agency for special cryptologic activities and for housing for personnel assigned to such activities.

(b) The Director of the National Security Agency, on behalf of the Secretary of Defense, may provide to certain civilian and military personnel of the Department of Defense who are assigned to special cryptologic activities outside the United States and who are designated by the Secretary of Defense for the purposes of this subsection—

(1) allowances and benefits—

(A) comparable to those provided by the Secretary of State to members of the Foreign Service under chapter 9 of title I of the Foreign Service Act of 1980 (22 U.S.C. 4081 et seq.) or any other provision of law; and

(B) in the case of selected personnel serving in circumstances similar to those in which personnel of the Central Intelligence Agency serve, comparable to those provided by the Director of Central Intelligence to personnel of the Central Intelligence Agency;

(2) housing (including heat, light, and household equipment) without cost to such personnel, if the Director of the National Security Agency, on behalf of the Secretary of Defense determines that it would be in the public interest to provide such housing; and

(3) special retirement accrual in the same manner provided in section 303 of the Central Intelligence Agency Retirement Act [50 U.S.C. § 2153] and in section 18 of the Central Intelligence Agency Act of 1949 [50 U.S.C. § 3518].

(c) The authority of the Director of the National Security Agency, on behalf of the Secretary of Defense, to make payments under subsections (a) and (b), and under contracts for leases entered into under subsection (a), is effective for any fiscal year only to the extent that appropriated funds are available for such purpose.

(d) Members of the Armed Forces may not receive benefits under both subsection (b)(1) and title 37, United States Code, for the same purpose. The Secretary of Defense shall prescribe such regulations as may be necessary to carry out this subsection.

(e) Regulations issued pursuant to subsection (b)(1) shall be submitted to the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate before such regulations take effect.

[LANGUAGE TRAINING AND CRYPTOLOGIC LINGUIST RESERVE PROGRAMS]

SEC. 10. [50 U.S.C. § 3608]

(a) The Director of the National Security Agency shall arrange for, and shall prescribe regulations concerning, language and language-related training programs for military and civilian cryptologic personnel. In establishing programs under this section for language and language-related training, the Director—

(1) may provide for the training and instruction to be furnished, including functional and geographic area specializations;

(2) may arrange for training and instruction through other Government agencies and, in any case in which appropriate training or instruction is unavailable through Government facilities, through nongovernmental facilities that furnish training and instruction useful in the fields of language and foreign affairs;

(3) may support programs that furnish necessary language and language-related skills, including, in any case in which appropriate programs are unavailable at Government facilities, support through contracts, grants, or cooperation with nongovernmental educational institutions; and

(4) may obtain by appointment or contract the services of individuals to serve as language instructors, linguists, or special language project personnel.

(b)(1) In order to maintain necessary capability in foreign language skills and related abilities needed by the National Security Agency, the Director, without

regard to subchapter IV of chapter 55 of title 5, United States Code, may provide special monetary or other incentives to encourage civilian cryptologic personnel of the Agency to acquire or retain proficiency in foreign languages or special related abilities needed by the Agency.

(2) In order to provide linguistic training and support for cryptologic personnel, the Director—

(A) may pay all or part of the tuition and other expenses related to the training of personnel who are assigned or detailed for language and language-related training, orientation, or instruction; and

(B) may pay benefits and allowances to civilian personnel in accordance with chapters 57 and 59 of title 5, United States Code, and to military personnel in accordance with chapter 7 of title 37, United States Code, and applicable provisions of title 10, United States Code, when such personnel are assigned to training at sites away from their designated duty station.

(c)(1) To the extent not inconsistent, in the opinion of the Secretary of Defense, with the operation of military cryptologic reserve units and in order to maintain necessary capability in foreign language skills and related abilities needed by the National Security Agency, the Director may establish a cryptologic linguist reserve. The cryptologic linguist reserve may consist of former or retired civilian or military cryptologic personnel of the National Security Agency and of other qualified individuals, as determined by the Director of the Agency. Each member of the cryptologic linguist reserve shall agree that, during any period of emergency (as determined by the Director), the member shall return to active civilian status with the National Security Agency and shall perform such linguistic or linguistic-related duties as the Director may assign.

(2) In order to attract individuals to become members of the cryptologic linguist reserve, the Director, without regard to subchapter IV of chapter 55 of title 5, United States Code, may provide special monetary incentives to individuals eligible to become members of the reserve who agree to become members of the cryptologic linguist reserve and to acquire or retain proficiency in foreign languages or special related abilities.

(3) In order to provide training and support for members of the cryptologic linguist reserve, the Director—

(A) may pay all or part of the tuition and other expenses related to the training of individuals in the cryptologic linguist reserve who are assigned or detailed for language and language-related training, orientation, or instruction; and

(B) may pay benefits and allowances in accordance with chapters 57 and 59 of title 5, United States Code, to individuals

in the cryptologic linguist reserve who are assigned to training at sites away from their homes or regular places of business.

- (d)(1) The Director, before providing training under this section to any individual, may obtain an agreement with that individual that—
- (A) in the case of current employees, pertains to continuation of service of the employee, and repayment of the expenses of such training for failure to fulfill the agreement, consistent with the provisions of section 4108 of title 5, United States Code; and
 - (B) in the case of individuals accepted for membership in the cryptologic linguist reserve, pertains to return to service when requested, and repayment of the expenses of such training for failure to fulfill the agreement, consistent with the provisions of section 4108 of title 5, United States Code.
- (2) The Director, under regulations prescribed under this section, may waive, in whole or in part, a right of recovery under an agreement made under this subsection if it is shown that the recovery would be against equity and good conscience or against the public interest.
- (e)(1) Subject to paragraph (2), the Director may provide to family members of military and civilian cryptologic personnel assigned to representational duties outside the United States, in anticipation of the assignment of such personnel outside the United States or while outside the United States, appropriate orientation and language training that is directly related to the assignment abroad.
- (2) Language training under paragraph (1) may not be provided to any individual through payment of the expenses of tuition or other cost of instruction at a non-Government educational institution unless appropriate instruction is not available at a Government facility.
- (f) The Director may waive the applicability of any provision of chapter 41 of title 5, United States Code, to any provision of this section if he finds that such waiver is important to the performance of cryptologic functions.
- (g) The authority of the Director to enter into contracts or to make grants under this section is effective for any fiscal year only to the extent that appropriated funds are available for such purpose.
- (h) Regulations issued pursuant to this section shall be submitted to the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate before such regulations take effect.
- (i) The Director of the National Security Agency, on behalf of the Secretary of Defense, may, without regard to section 4109(a)(2)(B) of title 5, United States Code, pay travel, transportation, storage, and subsistence expenses under chapter 57 of such title to civilian and military personnel of the Department of Defense who are assigned to duty outside the United States for a period of one year or

longer which involves cryptologic training, language training, or related disciplines.

[ENHANCEMENT OF SECURITY AUTHORITIES]

SEC. 11. [50 U.S.C. § 3609]

(a)(1) The Director of the National Security Agency may authorize agency personnel within the United States to perform the same functions as officers and agents of the Department of Homeland Security, as provided in section 1315(b)(2) of title 40, United States Code, with the powers set forth in that section, except that such personnel shall perform such functions and exercise such powers—

(A) at the National Security Agency Headquarters complex and at any facilities and protected property which are solely under the administration and control of, or are used exclusively by, the National Security Agency; and

(B) in the streets, sidewalks, and the open areas within the zone beginning at the outside boundary of such facilities or protected property and extending outward 500 feet.

(2) The performance of functions and exercise of powers under subparagraph (B) of paragraph (1) shall be limited to those circumstances where such personnel can identify specific and articulable facts giving such personnel reason to believe that the performance of such functions and exercise of such powers is reasonable to protect against physical damage or injury, or threats of physical damage or injury, to agency installations, property, or employees.

(3) Nothing in this subsection shall be construed to preclude, or limit in any way, the authority of any Federal, State, or local law enforcement agency, or any other Federal police or Federal protective service.

(4) The rules and regulations enforced by such personnel shall be the rules and regulations prescribed by the Director and shall only be applicable to the areas referred to in subparagraph (A) of paragraph (1).

(5) Agency personnel authorized by the Director under paragraph (1) may transport an individual apprehended under the authority of this section from the premises at which the individual was apprehended, as described in subparagraph (A) or (B) of paragraph (1), for the purpose of transferring such individual to the custody of law enforcement officials. Such transportation may be provided only to make a transfer of custody at a location within 30 miles of the premises described in subparagraphs (A) and (B) of paragraph (1).

(b) The Director of the National Security Agency is authorized to establish penalties for violations of the rules or regulations prescribed by the Director

under subsection (a). Such penalties shall not exceed those specified in section 1315(c)(2) of title 40, United States Code.

(c) Agency personnel designated by the Director of the National Security Agency under subsection (a) shall be clearly identifiable as United States Government security personnel while engaged in the performance of the functions to which subsection (a) refers.

(d)(1) Notwithstanding any other provision of law, agency personnel designated by the Director of the National Security Agency under subsection (a) shall be considered for purposes of chapter 171 of title 28, United States Code, or any other provision of law relating to tort liability, to be acting within the scope of their office or employment when such agency personnel take reasonable action, which may include the use of force, to—

(A) protect and individual in the presence of such agency personnel from a crime of violence;

(B) provide immediate assistance to an individual who has suffered or who is threatened with bodily harm;

(C) prevent the escape of any individual whom such agency personnel reasonably believe to have committed a crime of violence in the presence of such agency personnel; or

(D) transport an individual pursuant to subsection (a)(2).

(2) Paragraph (1) shall not affect the authorities of the Attorney General under section 2679 of title 28, United States Code.

(3) In this subsection, the term “crime of violence” as the meaning given that term in section 16 of title 18, United States Code.

[SENIOR CRYPTOLOGIC EXECUTIVE SERVICE]

SEC. 12. [50 U.S.C. § 3610]

(a)(1) The Secretary of Defense (or his designee) may by regulation establish a personnel system for senior civilian cryptologic personnel in the National Security Agency to be known as the Senior Cryptologic Executive Service. The regulations establishing the Senior Cryptologic Executive Service shall—

(A) meet the requirements set forth in section 3131 of title 5, United States Code, for the Senior Executive Service;

(B) provide that positions in the Senior Cryptologic Executive Service meet requirements that are consistent with the provisions of section 3132(a)(2) of such title;

(C) provide, without regard to section 2, rates of pay for the Senior Cryptologic Executive Service that are not in excess of the maximum rate or less than the minimum rate of basic pay established for the Senior Executive Service under section 5382 of such title, and that are adjusted at the same time and to the

same extent as rates of basic pay for the Senior Executive Service are adjusted;

(D) provide a performance appraisal system for the Senior Cryptologic Executive Service that conforms to the provisions of subchapter II of chapter 43 of such title;

(E) provide for removal consistent with section 3592 of such title, and removal or suspension consistent with subsections (a), (b), and (c) of section 7543 of such title (except that any hearing or appeal to which a member of the Senior Cryptologic Executive Service is entitled shall be held or decided pursuant to procedures established by regulations of the Secretary of Defense or his designee);

(F) permit the payment of performance awards to members of the Senior Cryptologic Executive Service consistent with the provisions applicable to performance awards under section 5384 of such title;

(G) provide that members of the Senior Cryptologic Executive Service may be granted sabbatical leaves consistent with the provisions of section 3396(c) of such title. [*sic*]

(H) provide for the recertification of members of the Senior Cryptologic Executive Service consistent with the provisions of section 3393a of such title.

(2) Except as otherwise provided in subsection (a), the Secretary of Defense (or his designee) may—

(A) make applicable to the Senior Cryptologic Executive Service any of the provisions of title 5, United States Code, applicable to applicants for or members of the Senior Executive Service; and

(B) appoint, promote, and assign individuals to positions established within the Senior Cryptologic Executive Service without regard to the provisions of title 5, United States Code, governing appointments and other personnel actions in the competitive service.

(3) The President, based on the recommendations of the Secretary of Defense, may award ranks to members of the Senior Cryptologic Executive Service in a manner consistent with the provisions of section 4507 of title 5, United States Code.

(4) Notwithstanding any other provision of this section, the Director of the National Security Agency may detail or assign any member of the Senior Cryptologic Executive Service to serve in a position outside the National Security Agency in which the member's expertise and experience may be of benefit to the National Security Agency or another Government agency. Any such member shall not by reason of such detail

or assignment lose any entitlement or status associated with membership in the Senior Cryptologic Executive Service.

(b) The Secretary of Defense (or his designee) may by regulation establish a merit pay system for such employees of the National Security Agency as the Secretary of Defense (or his designee) considers appropriate. The merit pay system shall be designed to carry out purposes consistent with those set forth in section 5401(a) of title 5, United States Code.

(c) Nothing in this section shall be construed to allow the aggregate amount payable to a member of the Senior Cryptologic Executive Service under this section during any fiscal year to exceed the annual rate payable for positions at level I of the Executive Schedule [5 U.S.C. § 5312] in effect at the end of such year.

[CRYPTOLOGIC RESEARCH GRANT PROGRAM]

SEC. 13. [50 U.S.C. § 3611]

(a) The Director of the National Security Agency may make grants to private individuals and institutions for the conduct of cryptologic research. An application for a grant under this section may not be approved unless the Director determines that the award of the grant would be clearly consistent with the national security.

(b) The grant program established by subsection (a) shall be conducted in accordance with the Federal Grant and Cooperative Agreement Act of 1977 (41 U.S.C. § 501 et seq.) to the extent that such Act is consistent with and in accordance with section 6 of this Act.

(c) The authority of the Director to make grants under this section is effective for any fiscal year only to the extent that appropriated funds are available for such purpose.

[AVAILABILITY OF APPROPRIATIONS]

SEC. 14. [50 U.S.C. § 3612]

Funds appropriated to an entity of the Federal Government other than an element of the Department of Defense that have been specifically appropriated for the purchase of cryptologic equipment, materials, or services with respect to which the National Security Agency has been designated as the central source of procurement for the Government shall remain available for a period of three fiscal years.

[MISUSE OF AGENCY NAME, INITIALS, OR SEAL]

SEC. 15. [50 U.S.C. § 3613]

(a) No person may, except with the written permission of the Director of the National Security Agency, knowingly use the words “National Security Agency”, the initials “NSA”, the seal of the National Security Agency, or any colorable imitation of such words, initials, or seal in connection with any merchandise, impersonation, solicitation, or commercial activity in a manner reasonably calculated to convey the impression that such use is approved, endorsed, or authorized by the National Security Agency.

(b) Whenever it appears to the Attorney General that any person is engaged or is about to engage in an act or practice which constitutes or will constitute conduct prohibited by subsection (a), the Attorney General may initiate a civil proceeding in a district court of the United States to enjoin such act or practice. Such court shall proceed as soon as practicable to the hearing and determination of such action and may, at any time before final determination, enter such restraining orders or prohibitions, or take such other action as is warranted, to prevent injury to the United States or to any person or class of persons for whose protection the action is brought.

[LOUIS STOKES EDUCATIONAL SCHOLARSHIP PROGRAM]

SEC. 16. [50 U.S.C. § 3614]

(a) The purpose of this section is to establish an undergraduate and graduate training program, which may lead to a baccalaureate or graduate degree, to facilitate the recruitment of individuals, particularly minority high school students, with a demonstrated capability to develop skills critical to the mission of the National Security Agency, including mathematics, computer science, engineering, and foreign languages.

(b) The Secretary of Defense is authorized, in his discretion, to assign civilians who may or may not be employees of the National Security Agency as students at accredited professional, technical, and other institutions of higher learning for training at the undergraduate or graduate level in skills critical to effective performance of the mission of the Agency.

(c) The National Security Agency may pay, directly or by reimbursement to program participants, expenses incident to assignments under subsection (b), in any fiscal year only to the extent that appropriated funds are available for such purpose.

(d)(1) To be eligible for assignment under subsection (b), a program participant must agree in writing –

(A) to continue in the service of the Agency for the period of the assignment and to complete the educational course of training for which the program participant is assigned;

(B) to continue in the service of the Agency following completion of the assignment for a period of one-and-a-half years for each year of the assignment or part thereof;

(C) to reimburse the United States for the total cost of education (excluding the program participant's pay and allowances) provided under this section to the program if, prior to the program participant's completing the educational course of training for which the program participant is assigned, the assignment or the program participant's employment with the Agency is terminated—

(i) by the Agency due to misconduct by the program participant;

(ii) by the program participant voluntarily; or

(iii) by the Agency for the failure of the program participant to maintain such level of academic standing in the educational course of training as the Director of the National Security Agency shall have specified in the agreement of the program participant under this subsection; and

(D) to reimburse the United States if, after completing the educational course of training for which the program participant is assigned, the program participant's employment with the Agency is terminated either by the Agency due to misconduct by the program participant or by the program participant voluntarily, prior to the program participant's completion of the service obligation period described in subparagraph (B), in an amount that bears the same ratio to the total cost of the education (excluding the program participant's pay and allowances) provided to the program participant as the unserved portion of the service obligation period described in subparagraph (B) bears to the total period of the service obligation described in subparagraph (B).

(2) Subject to paragraph (3), the obligation to reimburse the United States under an agreement described in paragraph (1), including interest due on such obligation, is for all purposes a debt owing the United States.

(3)(A) A discharge in bankruptcy under title 11, United States Code, shall not release a person from an obligation to reimburse the United States required under an agreement described in paragraph (1) if the final

decree of the discharge in bankruptcy is issued within five years after the last day of the combined period of service obligation described in subparagraphs (A) and (B) of paragraph (1).

(B) The Secretary of Defense may release a person, in whole or in part, from the obligation to reimburse the United States under an agreement described in paragraph (1) when, in his discretion, the Secretary determines that equity or the interests of the United States so require.

(C) The Secretary of Defense shall permit an [*sic*] program participant assigned under this section who, prior to commencing a second academic year of such assignment, voluntarily terminates the assignment or the program participant's employment with the Agency, to satisfy his obligation under an agreement described in paragraph (1) to reimburse the United States by reimbursement according to a schedule of monthly payments which results in completion of reimbursement by a date five years after the date of termination of the assignment or employment or earlier at the option of the program participant.

(e) Agency efforts to recruit individuals at educational institutions for participation in the undergraduate and graduate training program established by this section shall be made openly and according to the common practices of universities and employers recruiting at such institutions.

(f) Chapter 41 of title 5 and subsections (a) and (b) of section 3324 of title 31, United States Code, shall not apply with respect to this section.

(g) The Secretary of Defense may issue such regulations as may be necessary to implement this section.

(h) The undergraduate and graduate training program established under this section shall be known as the Louis Stokes Educational Scholarship Program.

[SEC. 17. Repealed.]

[TRANSPORTATION OF REMAINS OF CERTAIN EMPLOYEES]

SEC. 18. [50 U.S.C. § 3616]

(a) The Secretary of Defense may pay the expenses referred to in section 5742(b) of title 5, United States Code, in the case of any employee of the National Security Agency who dies while on a rotational tour of duty within the United States or while in transit to or from such tour of duty.

(b) For the purposes of this section, the term "rotational tour of duty", with respect to an employee, means a permanent change of station involving the transfer of the employee from the National Security Agency headquarters to another post of duty for a fixed period established by regulation to be followed at

the end of such period by a permanent change of station involving a transfer of the employee back to such headquarters.

[NATIONAL SECURITY AGENCY EMERGING TECHNOLOGIES PANEL]

SEC. 19. [50 U.S.C. § 3617]

(a) There is established the National Security Agency Emerging Technologies Panel. The Panel is a standing panel of the National Security Agency. The Panel shall be appointed by, and shall report directly to, the Director of the National Security Agency.

(b) The Panel shall study and assess, and periodically advise the Director on, the research, development, and application of existing and emerging science and technology advances, advances in encryption, and other topics.

(c) The Federal Advisory Committee Act (5 U.S.C. App.) shall not apply with respect to the Panel.

[COLLECTION OF SERVICE CHARGES FOR CERTIFICATION OR VALIDATION OF INFORMATION ASSURANCE PRODUCTS]

SEC. 20. [50 U.S.C. § 3618]

(a) The Director may collect charges for evaluating, certifying, or validating information assurance products under the National Information Assurance Program or successor program.

(b) The charges collected under subsection (a) shall be established through a public rulemaking process in accordance with Office of Management and Budget Circular No. A-25.

(c) Charges collected under subsection (a) shall not exceed the direct costs of the program referred to in that subsection.

(d) The appropriation or fund bearing the cost of the service for which charges are collected under the program referred to in subsection (a) may be reimbursed, or the Director may require advance payment subject to such adjustment on completion of the work as may be agreed upon.

(e) Amounts collected under this section shall be credited to the account or accounts from which costs associated with such amounts have been or will be incurred, to reimburse or offset the direct costs of the program referred to in subsection (a).

**[SENIOR CHIEF PETTY OFFICER SHANNON KENT AWARD FOR
DISTINGUISHED FEMALE PERSONNEL]**

SEC. 21.

(a) ESTABLISHMENT.—The Director of the National Security Agency shall establish an honorary award for the recognition of female personnel of the National Security Agency for distinguished career contributions in support of the mission of the Agency as civilian employees or members of the Armed Forces assigned to the Agency. The award shall be known as the ‘Senior Chief Petty Officer Shannon Kent Award’ and shall consist of a design determined appropriate by the Director.

(b) AWARD.—The Director shall award the Senior Chief Petty Officer Shannon Kent Award to female civilian employees, members of the Armed Forces, or former civilian employees or members, whom the Director determines meet the criteria under subsection (a).

**[CONGRESSIONAL NOTIFICATION OF INTELLIGENCE COLLECTION
ADJUSTMENTS]**

SEC. 22.

(a) NOTIFICATION.—Not later than 30 days after the date on which the Director of the National Security Agency determines the occurrence of an intelligence collection adjustment, the Director shall submit to the congressional intelligence committees, the Committee on Appropriations of the Senate, and the Committee on Appropriations of the House of Representatives a notification of the intelligence collection adjustment.

(b) DEFINITIONS.—In this section:

(1) CONGRESSIONAL INTELLIGENCE COMMITTEES.—The term ‘congressional intelligence committees’ has the meaning given that term in section 3 of the National Security Act of 1947 (50 U.S.C. 3003).

(2) INTELLIGENCE COLLECTION ADJUSTMENT.—The term ‘intelligence collection adjustment’ includes a change by the United States Government to a policy on intelligence collection or the prioritization thereof that results in a significant loss of intelligence.

TITLE 10, UNITED STATES CODE,
DEPARTMENT OF DEFENSE AUTHORITIES^[1]

TABLE OF CONTENTS

SUBTITLE A—GENERAL MILITARY LAW
PART I—ORGANIZATION AND GENERAL MILITARY POWERS
CHAPTER 4—OFFICE OF THE SECRETARY OF DEFENSE

SEC. 137. Under Secretary of Defense for Intelligence.

CHAPTER 21—DEPARTMENT OF DEFENSE INTELLIGENCE MATTERS

SUBCHAPTER I—GENERAL MATTERS

- SEC. 421. Funds for foreign cryptologic support.
SEC. 422. Use of funds for certain incidental purposes.
SEC. 423. Authority to use proceeds from counterintelligence operations of the military departments or the Defense Intelligence Agency.
SEC. 424. Disclosure of organizational and personnel information: exemption for specified intelligence agencies.
SEC. 425. Prohibition of unauthorized use of name, initials, or seal: specified intelligence agencies.
SEC. 426. Integration of Department of Defense intelligence, surveillance, and reconnaissance capabilities.
SEC. 427. Conflict Records Research Center.
SEC. 428. Defense industrial security.
SEC. 429. Appropriations for defense intelligence elements: accounts for transfers; transfer authority.
SEC. 430. Tactical exploitation of national capabilities executive agent.
SEC. 430a. Executive agent for management and oversight of alternative compensatory control measures.
SEC. 430b. Executive agent for open-source intelligence tools.

SUBCHAPTER II—INTELLIGENCE COMMERCIAL ACTIVITIES

- SEC. 431. Authority to engage in commercial activities as security for intelligence collection activities.
SEC. 432. Use, disposition, and auditing of funds.
SEC. 433. Relationship with other federal laws.

¹ Only select provisions are included, as reflected in the table of contents excerpt.

- SEC. 434. Reservation of defenses and immunities.
- SEC. 435. Limitations.
- SEC. 436. Regulations.
- SEC. 437. Congressional oversight.

CHAPTER 4—OFFICE OF THE SECRETARY OF DEFENSE

UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE

SEC. 137.

- (a) There is an Under Secretary of Defense for Intelligence and Security, appointed from civilian life by the President, by and with the advice and consent of the Senate. A person may not be appointed as Under Secretary within seven years after relief from active duty as a commissioned officer of a regular component of an armed force.
- (b) Subject to the authority, direction, and control of the Secretary of Defense, the Under Secretary of Defense for Intelligence and Security shall—
 - (1) have responsibility for the overall direction and supervision for policy, program planning and execution, and use of resources, for the activities of the Department of Defense that are part of the Military Intelligence Program;
 - (2) execute the functions for the National Intelligence Program of the Department of Defense under section 105 of the National Security Act of 1947 (50 U.S.C. 3038), as delegated by the Secretary of Defense;
 - (3) have responsibility for the overall direction and supervision for policy, program planning and execution, and use of resources, for personnel security, physical security, industrial security, and the protection of classified information and controlled unclassified information, related activities of the Department of Defense; and
 - (4) perform such duties and exercise such powers as the Secretary of Defense may prescribe in the area of intelligence.
- (c) The protection of privacy and civil liberties in accordance with Federal law and the regulations and directives of the Department of Defense shall be a top priority for the Under Secretary of Defense for Intelligence and Security.
- (d) The Under Secretary of Defense for Intelligence and Security takes precedence in the Department of Defense after the Under Secretary of Defense for Personnel and Readiness.

**CHAPTER 21—DEPARTMENT OF DEFENSE INTELLIGENCE
MATTERS**

SUBCHAPTER I—GENERAL MATTERS

FUNDS FOR FOREIGN CRYPTOLOGIC SUPPORT

SEC. 421.

- (a) The Secretary of Defense may use appropriated funds available to the Department of Defense for intelligence and communications purposes to pay for the expenses of arrangements with foreign countries for cryptologic support.
- (b) The Secretary of Defense may use funds other than appropriated funds to pay for the expenses of arrangements with foreign countries for cryptologic support without regard for the provisions of law relating to the expenditure of United States Government funds, except that—
- (1) no such funds may be expended, in whole or in part, by or for the benefit of the Department of Defense for a purpose for which Congress had previously denied funds; and
 - (2) proceeds from the sale of cryptologic items may be used only to purchase replacement items similar to the items that are sold; and
 - (3) the authority provided by this subsection may not be used to acquire items or services for the principal benefit of the United States.
- (c) Any funds expended under the authority of subsection (a) shall be reported to the Select Committee on Intelligence of the Senate and the Permanent Select Committee on Intelligence of the House of Representatives pursuant to the provisions of title V of the National Security Act of 1947 (50 U.S.C. § 3091 et seq.). Funds expended under the authority of subsection (b) shall be reported pursuant to procedures jointly agreed upon by such committees and the Secretary of Defense.

USE OF FUNDS FOR CERTAIN INCIDENTAL PURPOSES

SEC. 422.

- (a) **COUNTERINTELLIGENCE OFFICIAL RECEPTION AND REPRESENTATION EXPENSES.**—The Secretary of Defense may use funds available to the Department of Defense for counterintelligence programs to pay the expenses of hosting foreign officials in the United States under the auspices of the Department of Defense for consultation on counterintelligence matters.
- (b) **PROMOTIONAL ITEMS FOR RECRUITMENT PURPOSES.**—The Secretary of Defense may use funds available for an intelligence element of the Department of Defense to purchase promotional items of nominal value for use in the recruitment of individuals for employment by that element.

AUTHORITY TO USE PROCEEDS FROM COUNTERINTELLIGENCE OPERATIONS OF THE MILITARY DEPARTMENTS OR THE DEFENSE INTELLIGENCE AGENCY

SEC. 423.

(a) The Secretary of Defense may authorize, without regard to the provisions of section 3302 of title 31, use of proceeds from counterintelligence operations conducted by components of the military departments or the Defense Intelligence Agency to offset necessary and reasonable expenses, not otherwise prohibited by law, incurred in such operations, and to make exceptional performance awards to personnel involved in such operations, if use of appropriated funds to meet such expenses or to make such awards would not be practicable.

(b) As soon as the net proceeds from such counterintelligence operations are no longer necessary for the conduct of those operations, such proceeds shall be deposited into the Treasury as miscellaneous receipts.

(c) The Secretary of Defense shall establish policies and procedures to govern acquisition, use, management, and disposition of proceeds from counterintelligence operations conducted by components of the military departments or the Defense Intelligence Agency, including effective internal systems of accounting and administrative controls.

**DISCLOSURE OF ORGANIZATIONAL AND PERSONNEL INFORMATION:
EXEMPTION FOR SPECIFIED INTELLIGENCE AGENCIES**

SEC. 424.

(a) EXEMPTION FROM DISCLOSURE.—Except as required by the President or as provided in subsection (c), no provision of law shall be construed to require the disclosure of—

(1) the organization or any function of an organization of the Department of Defense named in subsection (b); or

(2) the number of persons employed by or assigned or detailed to any such organization or the name, official title, occupational series, grade, or salary of any such person.

(b) COVERED ORGANIZATIONS.—This section applies to the following organizations of the Department of Defense:

(1) The Defense Intelligence Agency.

(2) The National Reconnaissance Office.

(3) The National Geospatial-Intelligence Agency.

(c) PROVISION OF INFORMATION TO CONGRESS.—Subsection (a) does not apply with respect to the provision of information to Congress.

**PROHIBITION OF UNAUTHORIZED USE OF NAME, INITIALS, OR SEAL:
SPECIFIED INTELLIGENCE AGENCIES**

SEC. 425.

(a) PROHIBITION.—Except with the written permission of both the Secretary of Defense and the Director of National Intelligence, no person may knowingly use, in connection with any merchandise, retail product, impersonation, solicitation, or commercial activity in a manner reasonably calculated to convey the impression that such use is approved, endorsed, or authorized by the Secretary and the Director, any of the following (or any colorable imitation thereof):

(1) The words “Defense Intelligence Agency”, the initials “DIA”, or the seal of the Defense Intelligence Agency.

(2) The words “National Reconnaissance Office”, the initials “NRO”, or the seal of the National Reconnaissance Office.

(3) The words “National Imagery and Mapping Agency”, the initials “NIMA”, or the seal of the National Imagery and Mapping Agency.

(4) The words “Defense Mapping Agency”, the initials “DMA”, or the seal of the Defense Mapping Agency.

(5) The words “National Geospatial-Intelligence Agency”, the initials “NGA,” or the seal of the National Geospatial-Intelligence Agency.

(b) AUTHORITY TO ENJOIN VIOLATIONS.—Whenever it appears to the Attorney General that any person is engaged or is about to engage in an act or practice which constitutes or will constitute conduct prohibited by subsection (a), the Attorney General may initiate a civil proceeding in a district court of the United States to enjoin such act or practice. Such court shall proceed as soon as practicable to the hearing and determination of such action and may, at any time before final determination, enter such restraining orders or prohibitions, or take such other actions as is warranted, to prevent injury to the United States or to any person or class of persons for whose protection the action is brought.

**INTEGRATION OF DEPARTMENT OF DEFENSE INTELLIGENCE,
SURVEILLANCE, AND RECONNAISSANCE CAPABILITIES**

SEC. 426.

(a) ISR INTEGRATION COUNCIL.—

(1) The Under Secretary of Defense for Intelligence and Security shall establish an Intelligence, Surveillance, and Reconnaissance Integration Council—

(A) to assist the Secretary of Defense in carrying out the responsibilities of the Secretary under section 105(a) of the National Security Act of 1947 (50 U.S.C. 3038(a));

(B) to assist the Under Secretary with respect to matters relating to —

(i) integration of intelligence and counterintelligence capabilities and activities under section 137(b) of this title of the military departments, intelligence agencies of the Department of Defense, and relevant combatant commands; and

(ii) coordination of such developmental activities of such departments, agencies, and combatant commands; and

(C) to otherwise provide a means to facilitate such integration and coordination.

(2) The Council shall be composed of—

(A) the Under Secretary, who shall chair the Council;

(B) the directors of the intelligence agencies of the Department of Defense;

(C) the senior intelligence officers of the armed forces and the regional and functional combatant commands;

(D) the Director for Intelligence of the Joint Chiefs of Staff; and

(E) the Director for Operations of the Joint Chiefs of Staff.

(3) The Under Secretary of Defense for Intelligence shall invite the participation of the Director of National Intelligence (or a representative of the Director) in the proceedings of the Council.

(4) The Under Secretary of a military department may designate additional participants to attend the proceedings of the Council, as the Under Secretary determines appropriate.

(b) ANNUAL BRIEFING ON THE INTELLIGENCE AND COUNTERINTELLIGENCE REQUIREMENTS OF THE COMBATANT COMMANDS.—

(1) The Chairman of the Joint Chiefs of Staff shall provide to the congressional defense committees and the congressional intelligence committees a briefing on the following:

(A) The intelligence and counterintelligence requirements, by specific intelligence capability type, of each of the relevant combatant commands.

(B) For the year preceding the year in which the briefing is provided, the fulfillment rate for each of the relevant combatant commands of the validated intelligence and counterintelligence requirements, by specific intelligence capability type, of such combatant command.

(C) A risk analysis identifying the critical gaps and shortfalls in efforts to address operational and strategic requirements of the Department of Defense that would result from the failure to

fulfill the validated intelligence and counterintelligence requirements of the relevant combatant commands.

(D) A mitigation plan to balance and offset the gaps and shortfalls identified under subparagraph (C), including with respect to spaceborne, airborne, ground, maritime, and cyber intelligence, surveillance, and reconnaissance capabilities.

(E) For the year preceding the year in which the briefing is provided--

(i) the number of intelligence and counterintelligence requests of each commander of a relevant combatant command determined by the Joint Chiefs of Staff to be a validated requirement, and the total of capacity of such requests provided to each such commander;

(ii) with respect to such validated requirements--

(I) the quantity of intelligence and counterintelligence capabilities or activities, by specific intelligence capability type, that the Joint Chiefs of Staff requested each military department to provide; and

(II) the total of capacity of such requests so provided by each such military department; and

(iii) a qualitative assessment of the alignment of intelligence and counterintelligence capabilities and activities with the program of analysis for each combat support agency and intelligence center of a military service that is part of--

(I) the Defense Intelligence Enterprise; and

(II) the intelligence community.

(2) The Under Secretary of Defense for Intelligence and Security shall provide to the congressional defense committees and the congressional intelligence committees a briefing on short-, mid-, and long-term strategies to address the validated intelligence and counterintelligence requirements of the relevant combatant commands, including with respect to spaceborne, airborne, ground, maritime, and cyber intelligence, surveillance, and reconnaissance capabilities.

(3) The briefings required by paragraphs (1) and (2) shall be provided at the same time that the President's budget is submitted pursuant to section 1105(a) of title 31 for each of fiscal years 2021 through 2025.

(4) In this subsection:

(A) The term "congressional intelligence committees" has the meaning given that term in section 3 of the National Security Act of 1947 (50 U.S.C. 3003).

(B) The term “Defense Intelligence Enterprise” means the organizations, infrastructure, and measures, including policies, processes, procedures, and products, of the intelligence, counterintelligence, and security components of each of the following:

- (i) The Department of Defense.
- (ii) The Joint Staff.
- (iii) The combatant commands.
- (iv) The military departments.
- (v) Other elements of the Department of Defense that perform national intelligence, defense intelligence, intelligence-related, counterintelligence, or security functions.

(C) The term “fulfillment rate” means the percentage of combatant command intelligence and counterintelligence requirements satisfied by available, acquired, or realigned intelligence and counterintelligence capabilities or activities.

(D) The term “intelligence community” has the meaning given that term in section 3 of the National Security Act of 1947 (50 U.S.C. 3003).

CONFLICT RECORDS RESEARCH CENTER

SEC. 427.

(a) **CENTER AUTHORIZED.**—The Secretary of Defense may establish a center to be known as the “Conflict Records Research Center” (in this section referred to as the “Center”).

(b) **PURPOSES.**—The purposes of the Center shall be the following:

- (1) To establish a digital research database, including translations, and to facilitate research and analysis of records captured from countries, organizations, and individuals, now or once hostile to the United States, with rigid adherence to academic freedom and integrity.
- (2) Consistent with the protection of national security information, personally identifiable information, and intelligence sources and methods, to make a significant portion of these records available to researchers as quickly and responsibly as possible while taking into account the integrity of the academic process and risks to innocents or third parties.
- (3) To conduct and disseminate research and analysis to increase the understanding of factors related to international relations, counterterrorism, and conventional and unconventional warfare and, ultimately, enhance national security.

(4) To collaborate with members of academic and broad national security communities, both domestic and international, on research, conferences, seminars, and other information exchanges to identify topics of importance for the leadership of the United States Government and the scholarly community.

(c) CONCURRENCE OF THE DIRECTOR OF NATIONAL INTELLIGENCE.—The Secretary of Defense shall seek the concurrence of the Director of National Intelligence to the extent the efforts and activities of the Center involve the entities referred to in subsection (b)(4).

(d) SUPPORT FROM OTHER UNITED STATES GOVERNMENT DEPARTMENTS OR AGENCIES.—The head of any non-Department of Defense department or agency of the United States Government may—

(1) provide to the Secretary of Defense services, including personnel support, to support the operations of the Center; and

(2) transfer funds to the Secretary of Defense to support the operations of the Center.

(e) ACCEPTANCE OF GIFTS AND DONATIONS.—

(1) Subject to paragraph (3), the Secretary of Defense may accept from any source specified in paragraph (2) any gift or donation for purposes of defraying the costs or enhancing the operations of the Center.

(2) The sources specified in this paragraph are the following:

(A) The government of a State or a political subdivision of a State.

(B) The government of a foreign country.

(C) A foundation or other charitable organization, including a foundation or charitable organization that is organized or operates under the laws of a foreign country.

(D) Any source in the private sector of the United States or a foreign country.

(3) The Secretary may not accept a gift or donation under this subsection if acceptance of the gift or donation would compromise or appear to compromise—

(A) the ability of the Department of Defense, any employee of the Department, or any member of the armed forces to carry out the responsibility or duty of the Department in a fair and objective manner; or

(B) the integrity of any program of the Department or of any person involved in such a program.

(4) The Secretary shall provide written guidance setting forth the criteria to be used in determining the applicability of paragraph (3) to any proposed gift or donation under this subsection.

(f) **CREDITING OF FUNDS TRANSFERRED OR ACCEPTED.**—Funds transferred to or accepted by the Secretary of Defense under this section shall be credited to appropriations available to the Department of Defense for the Center, and shall be available for the same purposes, and subject to the same conditions and limitations, as the appropriations with which merged. Any funds so transferred or accepted shall remain available until expended.

(g) **DEFINITIONS.**—In this section:

(1) The term “captured record” means a document, audio file, video file, or other material captured during combat operations from countries, organizations, or individuals, now or once hostile to the United States.

(2) The term “gift or donation” means any gift or donation of funds, materials (including research materials), real or personal property, or services (including lecture services and faculty services).

DEFENSE INDUSTRIAL SECURITY

SEC. 428.

(a) **RESPONSIBILITY FOR DEFENSE INDUSTRIAL SECURITY.**—The Secretary of Defense shall be responsible for the protection of classified information disclosed to contractors of the Department of Defense.

(b) **CONSISTENCY WITH EXECUTIVE ORDERS AND DIRECTIVES.**—The Secretary shall carry out the responsibility assigned under subsection (a) in a manner consistent with Executive Order 12829 (or any successor order to such executive order) and consistent with policies relating to the National Industrial Security Program (or any successor to such program).

(c) **PERFORMANCE OF INDUSTRIAL SECURITY FUNCTIONS FOR OTHER AGENCIES.**—The Secretary may perform industrial security functions for other agencies of the Federal government upon request or upon designation of the Department of Defense as executive agent for the National Industrial Security Program (or any successor to such program).

(d) **REGULATIONS AND POLICY GUIDANCE.**—The Secretary shall prescribe, and from time to time revise, such regulations and policy guidance as are necessary to ensure the protection of classified information disclosed to contractors of the Department of Defense.

(e) **DEDICATION OF RESOURCES.**—The Secretary shall ensure that sufficient resources are provided to staff, train, and support such personnel as are necessary to fully protect classified information disclosed to contractors of the Department of Defense.

APPROPRIATIONS FOR DEFENSE INTELLIGENCE ELEMENTS: ACCOUNTS FOR TRANSFERS; TRANSFER AUTHORITY

SEC. 429.

(a) ACCOUNTS FOR APPROPRIATIONS FOR DEFENSE INTELLIGENCE ELEMENTS.—The Secretary of Defense may transfer appropriations of the Department of Defense which are available for the activities of Defense intelligence elements to an account or accounts established for receipt of such transfers. Each such account may also receive transfers from the Director of National Intelligence if made pursuant to Section 102A of the National Security Act of 1947 (50 U.S.C. 3024), and transfers and reimbursements arising from transactions, as authorized by law, between a Defense intelligence element and another entity. Appropriation balances in each such account may be transferred back to the account or accounts from which such appropriations originated as appropriation refunds.

(b) RECORDATION OF TRANSFERS.—Transfers made pursuant to subsection (a) shall be recorded as expenditure transfers.

(c) AVAILABILITY OF FUNDS.—Funds transferred pursuant to subsection (a) shall remain available for the same time period and for the same purpose as the appropriation from which transferred, and shall remain subject to the same limitations provided in the act making the appropriation.

(d) OBLIGATION AND EXPENDITURE OF FUNDS.—Unless otherwise specifically authorized by law, funds transferred pursuant to subsection (a) shall only be obligated and expended in accordance with chapter 15 of title 31 and all other applicable provisions of law.

(e) DEFENSE INTELLIGENCE ELEMENT DEFINED.—In this section, the term “Defense intelligence element” means any of the Department of Defense agencies, offices, and elements included within the definition of “intelligence community” under section 3(4) of the National Security Act of 1947 (50 U.S.C. 3003(4)).

TACTICAL EXPLOITATION OF NATIONAL CAPABILITIES EXECUTIVE AGENT

SEC. 430.

(a) DESIGNATION.—The Under Secretary of Defense for Intelligence shall designate a civilian employee of the Department or a member of the armed forces to serve as the Tactical Exploitation of National Capabilities Executive Agent.

(b) DUTIES.—The Executive Agent designated under subsection (a) shall—

- (1) report directly to the Under Secretary of Defense for Intelligence;
- (2) work with the combatant commands, military departments, and the intelligence community (as defined in section 3(4) of the National Security Act of 1947 (50 U.S.C. 3003(4))) to—

- (A) develop methods to increase warfighter effectiveness through the exploitation of national capabilities; and
- (B) promote cross-domain integration of such capabilities into military operations, training, intelligence, surveillance, and reconnaissance activities.

EXECUTIVE AGENT FOR MANAGEMENT AND OVERSIGHT OF ALTERNATIVE COMPENSATORY CONTROL MEASURES

SEC. 430a.

(a) **EXECUTIVE AGENT.**—The Secretary of Defense shall designate a senior official from among the personnel of the Department of Defense to act as the Department of Defense executive agent for the management and oversight of alternative compensatory control measures.

(b) **ROLES, RESPONSIBILITIES, AND AUTHORITIES.**—The Secretary shall prescribe the roles, responsibilities, and authorities of the executive agent designated under subsection (a). Such roles, responsibilities, and authorities shall include the development of an annual management and oversight plan for Department-wide accountability and reporting to the congressional defense committees.

EXECUTIVE AGENT FOR OPEN-SOURCE INTELLIGENCE TOOLS

SEC. 430b.

(a) **DESIGNATION.**—Not later than April 1, 2016, the Secretary of Defense shall designate a senior official of the Department of Defense to serve as the executive agent for the Department for open-source intelligence tools.

(b) **ROLES, RESPONSIBILITIES, AND AUTHORITIES.**—

- (1) Not later than July 1, 2016, in accordance with Directive 5101.1, the Secretary shall prescribe the roles, responsibilities, and authorities of the executive agent designated under subsection (a).
- (2) The roles and responsibilities of the executive agent designated under subsection (a) shall include the following:
 - (A) Developing and maintaining a comprehensive list of open-source intelligence tools and technical standards.
 - (B) Establishing priorities for the development, acquisition, and integration of open-source intelligence tools into the intelligence enterprise, and other command and control systems as needed.
 - (C) Certifying all open-source intelligence tools with respect to compliance with the standards required by the framework and guidance for the Intelligence Community Information

Technology Enterprise, the Defense Intelligence Information Enterprise, and the Joint Information Environment.

(D) Assessing and making recommendations regarding the protection of privacy in the acquisition, analysis, and dissemination of open-source information available around the world.

(E) Performing such other assessments or analyses as the Secretary considers appropriate.

(c) **SUPPORT WITHIN DEPARTMENT OF DEFENSE.**—In accordance with Directive 5101.1, the Secretary shall ensure that the military departments, the Defense Agencies, and other elements of the Department of Defense provide the executive agent designated under subsection (a) with the appropriate support and resources needed to perform the roles, responsibilities, and authorities of the executive agent.

(d) **DEFINITIONS.**—In this section:

(1) The term “Directive 5101.1” means Department of Defense Directive 5101.1, or any successor directive relating to the responsibilities of an executive agent of the Department of Defense.

(2) The term “executive agent” has the meaning given the term “DoD Executive Agent” in Directive 5101.1.

(3) The term “open-source intelligence tools” means tools for the systematic collection, processing, and analysis of publicly available information for known or anticipated intelligence requirements.

SUBCHAPTER II—INTELLIGENCE COMMERCIAL ACTIVITIES

AUTHORITY TO ENGAGE IN COMMERCIAL ACTIVITIES AS SECURITY FOR INTELLIGENCE COLLECTION ACTIVITIES

SEC. 431.

(a) **AUTHORITY.**—The Secretary of Defense, subject to the provisions of this subchapter, may authorize the conduct of those commercial activities necessary to provide security for authorized intelligence collection activities abroad undertaken by the Department of Defense. No commercial activity may be initiated pursuant to this subchapter after December 31, 2024.

(b) **INTERAGENCY COORDINATION AND SUPPORT.**—Any such activity shall—

- (1) be coordinated with, and (where appropriate) be supported by, the Director of the Central Intelligence Agency; and
- (2) to the extent the activity takes place within the United States, be coordinated with, and (where appropriate) be supported by, the Director of the Federal Bureau of Investigation.

(c) **DEFINITIONS.**—In this subchapter:

(1) The term “commercial activities” means activities that are conducted in a manner consistent with prevailing commercial practices and includes—

- (A) the acquisition, use, sale, storage and disposal of goods and services;
- (B) entering into employment contracts and leases and other agreements for real and personal property;
- (C) depositing funds into and withdrawing funds from domestic and foreign commercial business or financial institutions;
- (D) acquiring licenses, registrations, permits, and insurance; and
- (E) establishing corporations, partnerships, and other legal entities.

(2) The term “intelligence collection activities” means the collection of foreign intelligence and counterintelligence information.

USE, DISPOSITION, AND AUDITING OF FUNDS

SEC. 432.

(a) **USE OF FUNDS.**—Funds generated by a commercial activity authorized pursuant to this subchapter may be used to offset necessary and reasonable expenses arising from that activity. Use of such funds for that purpose shall be kept to the minimum necessary to conduct the activity concerned in a secure manner. Any funds generated by the activity in excess of those required for that purpose shall be deposited, as often as may be practicable, into the Treasury as miscellaneous receipts.

(b) **AUDITS.**—

(1) The Secretary of Defense shall assign an organization within the Department of Defense to have auditing responsibility with respect to activities authorized under this subchapter.

(2) That organization shall audit the use and disposition of funds generated by any commercial activity authorized under this subchapter not less often than annually. The results of all such audits shall be reported to the congressional defense committees and the congressional intelligence committees (as defined in section 437(c) of this title) by not later than December 31 of each year.

RELATIONSHIP WITH OTHER FEDERAL LAWS

SEC. 433.

(a) **IN GENERAL.**—Except as provided by subsection (b), a commercial activity conducted pursuant to this subchapter shall be carried out in accordance with applicable Federal law.

(b) AUTHORIZATION OF WAIVERS WHEN NECESSARY TO MAINTAIN SECURITY.—

(1) If the Secretary of Defense determines, in connection with a commercial activity authorized pursuant to section 431 of this title, that compliance with certain Federal laws or regulations pertaining to the management and administration of Federal agencies would create an unacceptable risk of compromise of an authorized intelligence activity, the Secretary may, to the extent necessary to prevent such compromise, waive compliance with such laws or regulations.

(2) Any determination and waiver by the Secretary under paragraph (1) shall be made in writing and shall include a specification of the laws and regulations for which compliance by the commercial activity concerned is not required consistent with this section.

(3) The authority of the Secretary under paragraph (1) may be delegated only to the Deputy Secretary of Defense, an Under Secretary of Defense, an Assistant Secretary of Defense, or a Secretary of a military department.

(c) FEDERAL LAWS AND REGULATIONS.—For purposes of this section, Federal laws and regulations pertaining to the management and administration of Federal agencies are only those Federal laws and regulations pertaining to the following:

(1) The receipt and use of appropriated and nonappropriated funds.

(2) The acquisition or management of property or services.

(3) Information disclosure, retention, and management.

(4) The employment of personnel.

(5) Payments for travel and housing.

(6) The establishment of legal entities or government instrumentalities.

(7) Foreign trade or financial transaction restrictions that would reveal the commercial activity as an activity of the United States Government.

RESERVATION OF DEFENSES AND IMMUNITIES

SEC. 434.

The submission to judicial proceedings in a State or other legal jurisdiction, in connection with a commercial activity undertaken pursuant to this subchapter, shall not constitute a waiver of the defenses and immunities of the United States.

LIMITATIONS

SEC. 435.

(a) LAWFUL ACTIVITIES.—Nothing in this subchapter authorizes the conduct of any intelligence activity that is not otherwise authorized by law or Executive order.

(b) DOMESTIC ACTIVITIES.—Personnel conducting commercial activity authorized by this subchapter may only engage in those activities in the United States to the extent necessary to support intelligence activities abroad.

(c) PROVIDING GOODS AND SERVICES TO THE DEPARTMENT OF DEFENSE.—Commercial activity may not be undertaken within the United States for the purpose of providing goods and services to the Department of Defense, other than as may be necessary to provide security for the activities subject to this subchapter.

(d) NOTICE TO UNITED STATES PERSONS.—

(1) In carrying out a commercial activity authorized under this subchapter, the Secretary of Defense may not permit an entity engaged in such activity to employ a United States person in an operational, managerial, or supervisory position, and may not assign or detail a United States person to perform operational, managerial, or supervisory duties for such an entity, unless that person is informed in advance of the intelligence security purpose of that activity.

(2) In this subsection, the term “United States person” means an individual who is a citizen of the United States or an alien lawfully admitted to the United States for permanent residence.

REGULATIONS

SEC. 436.

The Secretary of Defense shall prescribe regulations to implement the authority provided in this subchapter. Such regulations shall be consistent with this subchapter and shall at a minimum—

(1) specify all elements of the Department of Defense who are authorized to engage in commercial activities pursuant to this subchapter;

(2) require the personal approval of the Secretary or Deputy Secretary of Defense for all sensitive activities to be authorized pursuant to this subchapter;

(3) specify all officials who are authorized to grant waivers of laws or regulations pursuant to section 433 (b) of this title, or to approve the establishment or conduct of commercial activities pursuant to this subchapter;

(4) designate a single office within the Department of Defense to be responsible for the oversight of all activities authorized under this subchapter;

(5) require that each commercial activity proposed to be authorized under this subchapter be subject to appropriate legal review before the activity is authorized; and

(6) provide for appropriate internal audit controls and oversight for such activities.

CONGRESSIONAL OVERSIGHT

SEC. 437.

(a) **PROPOSED REGULATIONS.**—Copies of regulations proposed to be prescribed under section 436 of this title (including any proposed revision to such regulations) shall be submitted to the congressional defense committees and intelligence committees not less than 30 days before they take effect.

(b) **CURRENT INFORMATION.**—The Secretary of Defense shall ensure that congressional defense committees and the congressional intelligence committees are kept fully and currently informed of actions taken pursuant to this subchapter, including any significant anticipated activity to be authorized pursuant to this subchapter.

(c) **CONGRESSIONAL INTELLIGENCE COMMITTEES DEFINED.**—In this section, the term “congressional intelligence committees” has the meaning given the term in section 3 of the National Security Act of 1947 (50 U.S.C. 3003).

TITLE 10, CHAPTER 22, UNITED STATES CODE,
NATIONAL GEOSPATIAL-INTELLIGENCE
AGENCY AUTHORITIES^[1]

TABLE OF CONTENTS

SUBCHAPTER I—MISSIONS AND AUTHORITY

- SEC. 441. Establishment.
- SEC. 442. Missions.
- SEC. 443. Imagery intelligence and geospatial information: support for foreign countries, regional organizations, and security alliances.
- SEC. 444. Support from Central Intelligence Agency.

SUBCHAPTER II—MAPS, CHARTS, AND GEOMATICS PRODUCTS

- SEC. 451. Maps, charts, and books.
- SEC. 452. Pilot charts.
- SEC. 453. Sale of maps, charts, and navigational publications: prices; use of proceeds.
- SEC. 454. Exchange of mapping, charting, and geomatics data with foreign countries, international organizations, nongovernmental organizations, and academic institutions.
- SEC. 455. Maps, charts, and geomatics data: public availability; exceptions.
- SEC. 456. Civil actions barred.
- SEC. 457. Operational files previously maintained by or concerning activities of National Photographic Interpretation Center: authority to withhold from public disclosure.

SUBCHAPTER III—PERSONNEL MANAGEMENT

- SEC. 461. Management rights.
- SEC. 462. Financial assistance to certain employees in acquisition of critical skills.

SUBCHAPTER IV—DEFINITIONS

- SEC. 467. Definitions.

¹ Only select provisions are included, as reflected in the table of contents excerpt.

SUBCHAPTER I—MISSIONS AND AUTHORITY

ESTABLISHMENT

SEC. 441.

(a) **ESTABLISHMENT.**—The National Geospatial-Intelligence Agency is a combat support agency of the Department of Defense and has significant national missions.

(b) **DIRECTOR.**—

(1) The Director of the National Geospatial-Intelligence Agency is the head of the agency.

(2) Upon a vacancy in the position of Director, the Secretary of Defense shall recommend to the President an individual for appointment to the position.

(3) If an officer of the armed forces on active duty is appointed to the position of Director, the position shall be treated as having been designated by the President as a position of importance and responsibility for purposes of section 601 of this title and shall carry the grade of lieutenant general, or, in the case of an officer of the Navy, vice admiral.

(c) **DIRECTOR OF NATIONAL INTELLIGENCE COLLECTION TASKING**

AUTHORITY.—Unless otherwise directed by the President, the Director of National Intelligence shall have authority (except as otherwise agreed by the Director and the Secretary of Defense) to—

(1) approve collection requirements levied on national imagery collection assets;

(2) determine priorities for such requirements; and

(3) resolve conflicts in such priorities.

(d) **AVAILABILITY AND CONTINUED IMPROVEMENT OF IMAGERY INTELLIGENCE SUPPORT TO ALL-SOURCE ANALYSIS AND PRODUCTION FUNCTION.**—The Secretary of Defense, in consultation with the Director of National Intelligence, shall take all necessary steps to ensure the full availability and continued improvement of imagery intelligence support for all-source analysis and production.

MISSIONS

SEC. 442.

(a) **NATIONAL SECURITY MISSIONS.**—

(1) The National Geospatial-Intelligence Agency shall, in support of the national security objectives of the United States, provide geospatial intelligence consisting of the following:

- (A) Imagery.
- (B) Imagery intelligence.
- (C) Geospatial information.

(2)(A) As directed by the Director of National Intelligence, the National Geospatial-Intelligence Agency shall develop a system to facilitate the analysis, dissemination, and incorporation of likenesses, videos, and presentations produced by ground-based platforms, including handheld or clandestine photography taken by or on behalf of human intelligence collection organizations or available as open-source information, into the National System for Geospatial Intelligence.

(B) The authority provided by this paragraph does not include authority for the National Geospatial-Intelligence Agency to manage tasking of handheld or clandestine photography taken by or on behalf of human intelligence collection organizations.

(3) Geospatial intelligence provided in carrying out paragraphs (1) and (2) shall be timely, relevant, and accurate.

(b) NAVIGATION INFORMATION.—The National Geospatial-Intelligence Agency shall improve means of navigating vessels of the Navy and the merchant marine by providing, under the authority of the Secretary of Defense, accurate and inexpensive nautical charts, sailing directions, books on navigation, and manuals of instructions for the use of all vessels of the United States and of navigators generally.

(c) MAPS, CHARTS, ETC.—The National Geospatial-Intelligence Agency shall acquire, prepare, and distribute maps, safe-for-navigation charts and datasets, charts, books, and geomatics products as authorized under subchapter II of this chapter.

(d) NATIONAL MISSIONS.—The National Geospatial-Intelligence Agency also has national missions as specified in section 110(a) of the National Security Act of 1947 (50 U.S.C. 3045(a)).

(e) SYSTEMS.—The National Geospatial-Intelligence Agency may, in furtherance of a mission of the Agency, design, develop, deploy, operate, and maintain systems related to the processing and dissemination of imagery intelligence and geospatial information that may be transferred to, accepted or used by, or used on behalf of—

- (1) the armed forces, including any combatant command, component of a combatant command, joint task force, or tactical unit; or
- (2) any other department or agency of the United States.

(f) VALIDATION.—The National Geospatial-Intelligence Agency shall assist the Joint Chiefs of Staff, combatant commands, and the military departments in establishing, coordinating, consolidating, and validating mapping, charting, geomatics data, and safety of navigation capability requirements through a

formal process governed by the Joint Staff. Consistent with validated requirements, the National Geospatial-Intelligence Agency shall provide aeronautical and nautical charts that are safe for navigation, maps, books, datasets, models, and geomatics products.

**IMAGERY INTELLIGENCE AND GEOSPATIAL INFORMATION:
SUPPORT FOR FOREIGN COUNTRIES, REGIONAL ORGANIZATIONS, AND
SECURITY ALLIANCES**

SEC. 443.

(a) **USE OF APPROPRIATED FUNDS.**—The Director of the National Geospatial-Intelligence Agency may use appropriated funds available to the National Geospatial-Intelligence Agency to provide foreign countries, regional organizations with defense or security components, and security alliances of which the United States is a member with imagery intelligence and geospatial information support.

(b) **USE OF FUNDS OTHER THAN APPROPRIATED FUNDS.**—The Director may use funds other than appropriated funds to provide foreign countries with imagery intelligence and geospatial information support, notwithstanding provisions of law relating to the expenditure of funds of the United States, except that—

(1) no such funds may be expended, in whole or in part, by or for the benefit of the National Geospatial-Intelligence Agency for a purpose for which Congress had previously denied funds;

(2) proceeds from the sale of imagery intelligence or geospatial information items may be used only to purchase replacement items similar to the items that are sold; and

(3) the authority provided by this subsection may not be used to acquire items or services for the principal benefit of the United States.

(c) **ACCOMMODATION PROCUREMENTS.**—The authority under this section may be exercised to conduct accommodation procurements on behalf of foreign countries.

(d) **COORDINATION WITH DIRECTOR OF NATIONAL INTELLIGENCE.**—The Director of the Agency shall coordinate with the Director of National Intelligence any action under this section that involves imagery intelligence or intelligence products or involves providing support to an intelligence or security service of a foreign country.

SUPPORT FROM CENTRAL INTELLIGENCE AGENCY

SEC. 444.

(a) **SUPPORT AUTHORIZED.**—The Director of the Central Intelligence Agency may provide support in accordance with this section to the Director of the National Geospatial-Intelligence Agency. The Director of the National Geospatial-Intelligence Agency may accept support provided under this section.

(b) **ADMINISTRATIVE AND CONTRACT SERVICES.**—

(1) In furtherance of the national intelligence effort, the Director of the Central Intelligence Agency may provide administrative and contract services to the National Geospatial-Intelligence Agency as if that agency were an organizational element of the Central Intelligence Agency.

(2) Services provided under paragraph (1) may include the services of security police. For purposes of section 15 of the Central Intelligence Agency Act of 1949 (50 U.S.C. 3515), an installation of the National Geospatial-Intelligence Agency that is provided security police services under this section shall be considered an installation of the Central Intelligence Agency.

(3) Support provided under this subsection shall be provided under terms and conditions agreed upon by the Secretary of Defense and the Director of the Central Intelligence Agency.

(c) **DETAIL OF PERSONNEL.**—The Director of the Central Intelligence Agency may detail personnel of the Central Intelligence Agency indefinitely to the National Geospatial-Intelligence Agency without regard to any limitation on the duration of interagency details of Federal Government personnel.

(d) **REIMBURSABLE OR NONREIMBURSABLE SUPPORT.**—Support under this section may be provided and accepted on either a reimbursable basis or a nonreimbursable basis.

(e) **AUTHORITY TO TRANSFER FUNDS.**—

(1) The Director of the National Geospatial-Intelligence Agency may transfer funds available for that agency to the Director of the Central Intelligence Agency for the Central Intelligence Agency.

(2) The Director of the Central Intelligence Agency—

(A) may accept funds transferred under paragraph (1); and

(B) shall expend such funds, in accordance with the Central Intelligence Agency Act of 1949 (50 U.S.C. 3501 et seq.), to provide administrative and contract services or detail personnel to the National Geospatial-Intelligence Agency under this section.

SUBCHAPTER II—MAPS, CHARTS, AND GEOMATICS PRODUCTS

MAPS, CHARTS, BOOKS, AND DATASETS

SEC. 451.

The Secretary of Defense may—

- (1) have the National Geospatial-Intelligence Agency prepare nautical and aeronautical charts, topographic and geomatics maps, books, models, and datasets required in navigation and have those materials published and furnished to navigators; and
- (2) acquire (by purchase, lease, license, or barter) all necessary rights, including copyrights and other intellectual property rights, required to prepare, publish, and furnish to navigators the products described in paragraph (1).

PILOT CHARTS

SEC. 452.

- (a) There shall be conspicuously printed on pilot charts prepared in the National Geospatial-Intelligence Agency the following: “Prepared from data furnished by the National Geospatial-Intelligence Agency of the Department of Defense and by the Department of Commerce, and published at the National Geospatial-Intelligence Agency under the authority of the Secretary of Defense”.
- (b) The Secretary of Commerce shall furnish to the National Geospatial-Intelligence Agency, as quickly as possible, all meteorological information received by the Secretary that is necessary for, and of the character used in, preparing pilot charts.

**SALE OF MAPS, CHARTS, AND NAVIGATIONAL PUBLICATIONS:
PRICES; USE OF PROCEEDS**

SEC. 453.

- (a) **PRICES.**—All maps, charts, and other publications offered for sale by the National Geospatial-Intelligence Agency shall be sold at prices and under regulations that may be prescribed by the Secretary of Defense.
- (b) **USE OF PROCEEDS TO PAY FOREIGN LICENSING FEES.**—
 - (1) The Secretary of Defense may pay any NGA foreign data acquisition fee out of the proceeds of the sale of maps, charts, and other publications of the Agency, and those proceeds are hereby made available for that purpose.

(2) In this subsection, the term “NGA foreign data acquisition fee” means any licensing or other fee imposed by a foreign country or international organization for the acquisition or use of data or products by the National Geospatial-Intelligence Agency.

EXCHANGE OF MAPPING, CHARTING, AND GEOMATIC DATA WITH FOREIGN COUNTRIES, INTERNATIONAL ORGANIZATIONS, NONGOVERNMENTAL ORGANIZATIONS, AND ACADEMIC INSTITUTIONS

SEC. 454.

(a) FOREIGN COUNTRIES AND INTERNATIONAL ORGANIZATIONS.—The Secretary of Defense may authorize the National Geospatial-Intelligence Agency to exchange or furnish mapping, charting, and geomatics data, supplies and services to a foreign country or international organization pursuant to an agreement for the production or exchange of such data.

(b) NONGOVERNMENTAL ORGANIZATIONS AND ACADEMIC INSTITUTIONS.—The Secretary may authorize the National Geospatial-Intelligence Agency to exchange or furnish mapping, charting, and geomatics data, supplies, and services relating to areas outside of the United States to a nongovernmental organization or an academic institution engaged in geospatial information research or production of such areas pursuant to an agreement for the production or exchange of such data.

MAPS, CHARTS, AND GEOMATIC DATA: PUBLIC AVAILABILITY; EXCEPTIONS

SEC. 455.

(a) The National Geospatial-Intelligence Agency shall offer for sale maps and charts at scales of 1:500,000 and smaller, except those withheld in accordance with subsection (b) or those specifically authorized under criteria established by Executive order to be kept secret in the interest of national defense or foreign policy and in fact properly classified pursuant to such Executive order.

(b)(1) Notwithstanding any other provision of law, the Secretary of Defense may withhold from public disclosure any geomatics product in the possession of, or under the control of, the Department of Defense—

(A) that was obtained or produced, or that contains information that was provided, pursuant to an international agreement that restricts disclosure of such product or information to government officials of the agreeing parties or that restricts use of such product or information to government purposes only;

(B) that contains information that the Secretary of Defense has determined in writing would, if disclosed, reveal sources and

methods, or capabilities, used to obtain source material for production of the geomatics product; or
(C) that contains information that the Director of the National Geospatial-Intelligence Agency has determined in writing would, if disclosed, jeopardize or interfere with ongoing military or intelligence operations, reveal military operational or contingency plans, or reveal, jeopardize, or compromise military or intelligence capabilities.

(2) In this subsection, the term “geomatics product” means imagery, imagery intelligence, or geospatial information.

(c)(1) Regulations to implement this section (including any amendments to such regulations) shall be published in the Federal Register for public comment for a period of not less than 30 days before they take effect.

(2) Regulations under this section shall address the conditions under which release of geomatics products authorized under subsection (b) to be withheld from public disclosure would be appropriate—

(A) in the case of allies of the United States; and

(B) in the case of qualified United States contractors (including contractors that are small business concerns) who need such products for use in the performance of contracts with the United States.

CIVIL ACTIONS BARRED

SEC. 456.

No civil action may be brought against the United States on the basis of the content of geospatial information prepared or disseminated by the National Geospatial-Intelligence Agency.

OPERATIONAL FILES PREVIOUSLY MAINTAINED BY OR CONCERNING ACTIVITIES OF NATIONAL PHOTOGRAPHIC INTERPRETATION CENTER: AUTHORITY TO WITHHOLD FROM PUBLIC DISCLOSURE

SEC. 457.

(a) **AUTHORITY.**—The Secretary of Defense may withhold from public disclosure operational files described in subsection (b) to the same extent that operational files may be withheld under section 701 of the National Security Act of 1947 (50 U.S.C. 3431).

(b) **COVERED OPERATIONAL FILES.**—The authority under subsection (a) applies to operational files in the possession of the National Geospatial-Intelligence Agency that—

(1) as of September 22, 1996, were maintained by the National Photographic Interpretation Center; or

(2) concern the activities of the Agency that, as of such date, were performed by the National Photographic Interpretation Center.

(c) OPERATIONAL FILES DEFINED.—In this section, the term “operational files” has the meaning given that term in section 701(b) of the National Security Act of 1947 (50 U.S.C. 3141(b)).

SUBCHAPTER III—PERSONNEL MANAGEMENT

MANAGEMENT RIGHTS

SEC. 461.

(a) SCOPE.—If there is no obligation under the provisions of chapter 71 of title 5 for the head of an agency of the United States to consult or negotiate with a labor organization on a particular matter by reason of that matter being covered by a provision of law or a Governmentwide regulation, the Director of the National Geospatial-Intelligence Agency is not obligated to consult or negotiate with a labor organization on that matter even if that provision of law or regulation is inapplicable to the National Geospatial-Intelligence Agency.

(b) BARGAINING UNITS.—The Director of the National Geospatial-Intelligence Agency shall accord exclusive recognition to a labor organization under section 7111 of title 5 only for a bargaining unit that was recognized as appropriate for the Defense Mapping Agency on September 30, 1996.

(c) TERMINATION OF BARGAINING UNIT COVERAGE OF POSITION MODIFIED TO AFFECT NATIONAL SECURITY DIRECTLY.—

(1) If the Director of the National Geospatial-Intelligence Agency determines that the responsibilities of a position within a collective bargaining unit should be modified to include intelligence, counterintelligence, investigative, or security duties not previously assigned to that position and that the performance of the newly assigned duties directly affects the national security of the United States, then, upon such a modification of the responsibilities of that position, the position shall cease to be covered by the collective bargaining unit and the employee in that position shall cease to be entitled to representation by a labor organization accorded exclusive recognition for that collective bargaining unit.

(2) A determination described in paragraph (1) that is made by the Director of the National Geospatial-Intelligence Agency may not be

reviewed by the Federal Labor Relations Authority or any court of the United States.

**FINANCIAL ASSISTANCE TO CERTAIN EMPLOYEES IN
ACQUISITION OF CRITICAL SKILLS**

SEC. 462.

The Secretary of Defense may establish an undergraduate training program with respect to civilian employees of the National Geospatial-Intelligence Agency that is similar in purpose, conditions, content, and administration to the program established by the Secretary of Defense under section 16 of the National Security Agency Act of 1959 (50 U.S.C. 3614) for civilian employees of the National Security Agency.

SUBCHAPTER IV—DEFINITIONS

DEFINITIONS

SEC. 467.

In this chapter:

(1) The term “function” means any duty, obligation, responsibility, privilege, activity, or program.

(2)(A) The term “imagery” means, except as provided in subparagraph (B), a likeness or presentation of any natural or manmade feature or related object or activity and the positional data acquired at the same time the likeness or representation was acquired, including—

(i) products produced by space-based national intelligence reconnaissance systems; and

(ii) likenesses or presentations produced by satellites, airborne platforms, unmanned aerial vehicles, or other similar means.

(B) Such term does not include handheld or clandestine photography taken by or on behalf of human intelligence collection organizations.

(3) The term “imagery intelligence” means the technical, geographic, and intelligence information derived through the interpretation or analysis of imagery and collateral materials.

(4) The term “geospatial information” means information that identifies the geographic location and characteristics of natural or constructed features and boundaries on or about the earth and includes—

(A) statistical data and information derived from, among other things, remote sensing, mapping, and surveying technologies; and

(B) mapping, charting, geomatics data, and related products and services.

(5) The term “geospatial intelligence” means the exploitation and analysis of imagery and geospatial information to describe, assess, and visually depict physical features and geographically referenced activities on or about the earth. Geospatial intelligence consists of imagery, imagery intelligence, and geospatial information.

HOMELAND SECURITY ACT OF 2002^[1]

[Public Law 107-296; 116 STAT. 2135; November 25, 2002]

AN ACT To establish the Department of Homeland Security, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SHORT TITLE; TABLE OF CONTENTS

SECTION 1. [6 U.S.C. § 101 note]

(a) SHORT TITLE.—This Act may be cited as the “Homeland Security Act of 2002”.

(b) TABLE OF CONTENTS.—The table of contents for this Act is as follows:

SEC. 1. Short title; table of contents.

SEC. 2. Definitions.

TITLE I—DEPARTMENT OF HOMELAND SECURITY

SEC. 101. Executive department; mission.

SEC. 102. Secretary; functions.

SEC. 103. Other officers.

TITLE II—INFORMATION ANALYSIS

SUBTITLE A—INFORMATION AND ANALYSIS; ACCESS TO INFORMATION

SEC. 201. Information and Analysis.

SEC. 202. Access to information.

SEC. 203. Homeland Security Advisory System.

SEC. 204. Homeland security information sharing.

SEC. 205. Comprehensive information technology network architecture.

SEC. 206. Coordination with information sharing environment.

SEC. 207. Intelligence components.

SEC. 208. Training for employees of intelligence components.

SEC. 209. Intelligence training development for State and local government officials.

¹ Only select provisions are included, as reflected in the table of contents excerpt.

HOMELAND SECURITY ACT OF 2002

- SEC. 210. Information sharing incentives.
- SEC. 210A. Department of Homeland Security State, Local, and Regional Information Fusion Center Initiative.
- SEC. 210B. Homeland Security Information Sharing Fellows Program.
- SEC. 210E. Classified Information Advisory Officer.

TITLE V—NATIONAL EMERGENCY MANAGEMENT

- SEC. 515. National Operations Center.

TITLE VIII—COORDINATION WITH NON-FEDERAL ENTITIES; INSPECTOR GENERAL; UNITED STATES SECRET SERVICE; COAST GUARD; GENERAL PROVISIONS

SUBTITLE A—COORDINATION WITH NON-FEDERAL ENTITIES

- SEC. 801. Office for State and Local Government Coordination.

SUBTITLE I—INFORMATION SHARING

- SEC. 891. Short title; findings; and sense of Congress.
- SEC. 892. Facilitating homeland security information sharing procedures.
- SEC. 893. Report.
- SEC. 894. Authorization of appropriations.

TITLE XIII—FEDERAL WORKFORCE IMPROVEMENT

SUBTITLE D—ACADEMIC TRAINING

- SEC. 1333. Intelligence and Cybersecurity Diversity Fellowship Program.

TITLE XXII—CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

SUBTITLE A—CYBERSECURITY AND INFRASTRUCTURE SECURITY

- SEC. 2209. National cybersecurity and communications integration center.
- SEC. 2210. Cybersecurity plans.
- SEC. 2212. Clearances.
- SEC. 2214. National Asset Database.
- SEC. 2215. Joint cyber planning office.

DEFINITIONS

SEC. 2. [6 U.S.C. § 101]

In this Act, the following definitions apply:

- (1) Each of the terms “American homeland” and “homeland” means the United States.
- (2) The term “appropriate congressional committee” means any committee of the House of Representatives or the Senate having legislative or oversight jurisdiction under the Rules of the House of Representatives or the Senate, respectively, over the matter concerned.
- (3) The term “assets” includes contracts, facilities, property, records, unobligated or unexpended balances of appropriations, and other funds or resources (other than personnel).
- (4) The term “critical infrastructure” has the meaning given that term in section 1016(e) of Public Law 107-56 (42 U.S.C. 5195c(e)).
- (5) The term “Department” means the Department of Homeland Security.
- (6) The term “emergency response providers” includes Federal, State, and local governmental and nongovernmental emergency public safety, fire, law enforcement, emergency response, emergency medical (including hospital emergency facilities), and related personnel, agencies, and authorities.
- (7) The term “EMP” means an electromagnetic pulse caused by a nuclear device or nonnuclear device, including such a pulse caused by an act of terrorism.
- (8) The term “executive agency” means an executive agency and a military department, as defined, respectively, in sections 105 and 102 of title 5, United States Code.
- (9) The term “functions” includes authorities, powers, rights, privileges, immunities, programs, projects, activities, duties, and responsibilities.
- (10) The term “GMD” means a geomagnetic disturbance caused by a solar storm or another naturally occurring phenomenon.
- (11) The term “intelligence component of the Department” means any element or entity of the Department that collects, gathers, processes, analyzes, produces, or disseminates intelligence information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information, or national intelligence, as defined under section 3(5) of the National Security Act of 1947 (50 U.S.C. 401a(5)), except—
 - (A) the United States Secret Service; and
 - (B) the Coast Guard, when operating under the direct authority of the Secretary of Defense or Secretary of the Navy pursuant to section 3 of title 14, United States Code, except that nothing in this paragraph shall affect or diminish the authority and responsibilities of the Commandant

of the Coast Guard to command or control the Coast Guard as an armed force or the authority of the Director of National Intelligence with respect to the Coast Guard as an element of the intelligence community (as defined under section 3(4) of the National Security Act of 1947 (50 U.S.C. 401a(4)).

- (12) The term “key resources” means publicly or privately controlled resources essential to the minimal operations of the economy and government.
- (13) The term “local government” means—
- (A) a county, municipality, city, town, township, local public authority, school district, special district, intrastate district, council of governments (regardless of whether the council of governments is incorporated as a nonprofit corporation under State law), regional or interstate government entity, or agency or instrumentality of a local government;
 - (B) an Indian tribe or authorized tribal organization, or in Alaska a Native village or Alaska Regional Native Corporation; and
 - (C) a rural community, unincorporated town or village, or other public entity.
- (14) The term “major disaster” has the meaning given in section 102(2) of the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5122).
- (15) The term “personnel” means officers and employees.
- (16) The term “Secretary” means the Secretary of Homeland Security.
- (17) The term “State” means any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, Guam, American Samoa, the Commonwealth of the Northern Mariana Islands, and any possession of the United States.
- (18) The term “terrorism” means any activity that—
- (A) involves an act that—
 - (i) is dangerous to human life or potentially destructive of critical infrastructure or key resources; and
 - (ii) is a violation of the criminal laws of the United States or of any State or other subdivision of the United States; and
 - (B) appears to be intended—
 - (i) to intimidate or coerce a civilian population;
 - (ii) to influence the policy of a government by intimidation or coercion; or
 - (iii) to affect the conduct of a government by mass destruction, assassination, or kidnapping.
- (19)(A) The term “United States”, when used in a geographic sense, means any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, Guam, American Samoa, the Commonwealth of the

Northern Mariana Islands, any possession of the United States, and any waters within the jurisdiction of the United States.

(B) Nothing in this paragraph or any other provision of this chapter shall be construed to modify the definition of “United States” for the purposes of the Immigration and Nationality Act or any other immigration or nationality law.

(20) The term “voluntary preparedness standards” means a common set of criteria for preparedness, disaster management, emergency management, and business continuity programs, such as the American National Standards Institute’s National Fire Protection Association Standard on Disaster/Emergency Management and Business Continuity Programs (ANSI/NFPA 1600).

TITLE I—DEPARTMENT OF HOMELAND SECURITY

EXECUTIVE DEPARTMENT; MISSION

SEC. 101. [6 U.S.C. § 111]

(a) ESTABLISHMENT.—There is established a Department of Homeland Security, as an executive department of the United States within the meaning of title 5, United States Code.

(b) MISSION.—

(1) IN GENERAL.—The primary mission of the Department is to—

- (A) prevent terrorist attacks within the United States;
- (B) reduce the vulnerability of the United States to terrorism;
- (C) minimize the damage, and assist in the recovery, from terrorist attacks that do occur within the United States;
- (D) carry out all functions of entities transferred to the Department, including by acting as a focal point regarding natural and manmade crises and emergency planning;
- (E) ensure that the functions of the agencies and subdivisions within the Department that are not related directly to securing the homeland are not diminished or neglected except by a specific explicit Act of Congress;
- (F) ensure that the overall economic security of the United States is not diminished by efforts, activities, and programs aimed at securing the homeland;
- (G) monitor connections between illegal drug trafficking and terrorism, coordinate efforts to sever such connections, and otherwise contribute to efforts to interdict illegal drug trafficking; and

(H) monitor connections between illegal drug trafficking and terrorism, coordinate efforts to sever such connections, and otherwise contribute to efforts to interdict illegal drug trafficking.

(2) **RESPONSIBILITY FOR INVESTIGATING AND PROSECUTING TERRORISM.**—Except as specifically provided by law with respect to entities transferred to the Department under this Act, primary responsibility for investigating and prosecuting acts of terrorism shall be vested not in the Department, but rather in Federal, State, and local law enforcement agencies with jurisdiction over the acts in question.

SECRETARY; FUNCTIONS

SEC. 102. [6 U.S.C. § 112]

(a) **SECRETARY.**—

(1) **IN GENERAL.**—There is a Secretary of Homeland Security, appointed by the President, by and with the advice and consent of the Senate.

(2) **HEAD OF DEPARTMENT.**—The Secretary is the head of the Department and shall have direction, authority, and control over it.

(3) **FUNCTIONS VESTED IN SECRETARY.**—All functions of all officers, employees, and organizational units of the Department are vested in the Secretary.

(b) **FUNCTIONS.**—The Secretary—

(1) except as otherwise provided by this Act, may delegate any of the Secretary's functions to any officer, employee, or organizational unit of the Department;

(2) shall have the authority to make contracts, grants, and cooperative agreements, and to enter into agreements with other executive agencies, as may be necessary and proper to carry out the Secretary's responsibilities under this Act or otherwise provided by law; and

(3) shall take reasonable steps to ensure that information systems and databases of the Department are compatible with each other and with appropriate databases of other Departments.

(c) **COORDINATION WITH NON-FEDERAL ENTITIES.**—With respect to homeland security, the Secretary shall coordinate through the Office of State and Local Coordination (established under section 801) (including the provision of training and equipment) with State and local government personnel, agencies, and authorities, with the private sector, and with other entities, including by:

(1) coordinating with State and local government personnel, agencies, and authorities, and with the private sector, to ensure adequate planning, equipment, training, and exercise activities;

(2) coordinating and, as appropriate, consolidating, the Federal Government's communications and systems of communications relating to homeland security with State and local government personnel, agencies, and authorities, the private sector, other entities, and the public; and

(3) distributing or, as appropriate, coordinating the distribution of, warnings and information to State and local government personnel, agencies, and authorities and to the public.

(d) MEETINGS OF NATIONAL SECURITY COUNCIL.—The Secretary may, subject to the direction of the President, attend and participate in meetings of the National Security Council.

(e) ISSUANCE OF REGULATIONS.—The issuance of regulations by the Secretary shall be governed by the provisions of chapter 5 of title 5, United States Code, except as specifically provided in this Act, in laws granting regulatory authorities that are transferred by this Act, and in laws enacted after the date of enactment of this Act.

(f) SPECIAL ASSISTANT TO THE SECRETARY.—The Secretary shall appoint a Special Assistant to the Secretary who shall be responsible for—

(1) creating and fostering strategic communications with the private sector to enhance the primary mission of the Department to protect the American homeland;

(2) advising the Secretary on the impact of the Department's policies, regulations, processes, and actions on the private sector;

(3) interfacing with other relevant Federal agencies with homeland security missions to assess the impact of these agencies' actions on the private sector;

(4) creating and managing private sector advisory councils composed of representatives of industries and associations designated by the Secretary to—

(A) advise the Secretary on private sector products, applications, and solutions as they relate to homeland security challenges;

(B) advise the Secretary on homeland security policies, regulations, processes, and actions that affect the participating industries and associations; and

(C) advise the Secretary on private sector preparedness issues, including effective methods for—

(i) promoting voluntary preparedness standards to the private sector; and

(ii) assisting the private sector in adopting voluntary preparedness standards;

(5) working with Federal laboratories, federally funded research and development centers, other federally funded organizations, academia, and the private sector to develop innovative approaches to address homeland security challenges to produce and deploy the best available technologies for homeland security missions;

(6) promoting existing public-private partnerships and developing new public-private partnerships to provide for collaboration and mutual support to address homeland security challenges;

(7) assisting in the development and promotion of private sector best practices to secure critical infrastructure;

(8) providing information to the private sector regarding voluntary preparedness standards and the business justification for preparedness and promoting to the private sector the adoption of voluntary preparedness standards;

(9) coordinating industry efforts, with respect to functions of the Department of Homeland Security, to identify private sector resources and capabilities that could be effective in supplementing Federal, State, and local government agency efforts to prevent or respond to a terrorist attack;

(10) coordinating with the Commissioner of U.S. Customs and Border Protection and the Assistant Secretary for Trade Development of the Department of Commerce on issues related to the travel and tourism industries; and

(11) consulting with the Office of State and Local Government Coordination and Preparedness on all matters of concern to the private sector, including the tourism industry.

(g) **STANDARDS POLICY.**—All standards activities of the Department shall be conducted in accordance with section 12(d) of the National Technology Transfer Advancement Act of 1995 (15 U.S.C. § 272 note) and Office of Management and Budget Circular A-119.

(h) **PLANNING REQUIREMENTS.**—The Secretary shall ensure the head of each office and component of the Department takes into account the needs of children, including children within underserved communities, in mission planning and mission execution. In furtherance of this subsection, the Secretary shall require each such head to seek, to the extent practicable, advice and feedback from organizations representing the needs of children. The Federal Advisory Committee Act (5 U.S.C. App.) shall not apply whenever such advice or feedback is sought in accordance with this subsection.

OTHER OFFICERS

SEC. 103. [6 U.S.C. § 113]

(a) **DEPUTY SECRETARY; UNDER SECRETARIES.**—

(1) **IN GENERAL.**—Except as provided under paragraph (2), there are the following officers, appointed by the President, by and with the advice and consent of the Senate:

(A) A Deputy Secretary of Homeland Security, who shall be the Secretary's first assistant for purposes of subchapter III of chapter 33 of title 5, United States Code.

(B) An Under Secretary for Science and Technology.

(C) A Commissioner of U.S. Customs and Border Protection.

(D) An Administrator of the Federal Emergency Management Agency.

(E) A Director of the Bureau of Citizenship and Immigration Services.

(F) An Under Secretary for Management, who shall be first assistant to the Deputy Secretary of Homeland Security for purposes of subchapter III of chapter 33 of title 5, United States Code.

(G) A Director of U.S. Immigration and Customs Enforcement.

(H) An Under Secretary responsible for overseeing critical infrastructure protection, cybersecurity, and other related programs of the Department.

(I) Not more than 12 Assistant Secretaries.

(J) A General Counsel, who shall be the chief legal officer of the Department.

(K) An Under Secretary for Strategy, Policy, and Plans.

(2) **ASSISTANT SECRETARIES.**—If any of the Assistant Secretaries referred to under paragraph (1)(I) is designated to be the Assistant Secretary for Health Affairs, the Assistant Secretary for Legislative Affairs, or the Assistant Secretary for Public Affairs, that Assistant Secretary shall be appointed by the President without the advice and consent of the Senate.

(b) **INSPECTOR GENERAL.**—There shall be in the Department an Office of Inspector General and an Inspector General at the head of such office, as provided in chapter 4 of title 5, United States Code.

(c) **COMMANDANT OF THE COAST GUARD.**—To assist the Secretary in the performance of the Secretary's functions, there is a Commandant of the Coast Guard, who shall be appointed as provided in section 44 of title 14, United States Code, and who shall report directly to the Secretary. In addition to such duties as

may be provided in this chapter and as assigned to the Commandant by the Secretary, the duties of the Commandant shall include those required by section 2 of title 14, United States Code.

(d) OTHER OFFICERS.—To assist the Secretary in the performance of the Secretary's functions, there are the following officers, appointed by the President:

- (1) A Director of the Secret Service.
- (2) A Chief Information Officer.
- (3) An Officer for Civil Rights and Civil Liberties.
- (4) A Director for Domestic Nuclear Detection.
- (5) Any Director of a Joint Task Force under section 348 of this title.

(e) CHIEF FINANCIAL OFFICER.—There shall be in the Department a Chief Financial Officer, as provided in chapter 9 of title 31, United States Code.

(f) PERFORMANCE OF SPECIFIC FUNCTIONS.—Subject to the provisions of this chapter, every officer of the Department shall perform the functions specified by law for the official's office or prescribed by the Secretary.

(g) VACANCIES.—

(1) ABSENCE, DISABILITY, OR VACANCY OF SECRETARY OR DEPUTY SECRETARY.—Notwithstanding chapter 33 of title 5, United States Code, the Under Secretary for Management shall serve as the Acting Secretary if by reason of absence, disability, or vacancy in office, neither the Secretary nor Deputy Secretary is available to exercise the duties of the Office of the Secretary.

(2) FURTHER ORDER OF SUCCESSION.—Notwithstanding chapter 33 of title 5, United States Code, the Secretary may designate such other officers of the Department in further order of succession to serve as Acting Secretary.

(3) NOTIFICATION OF VACANCIES.—The Secretary shall notify the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives of any vacancies that require notification under sections 3345 through 3349d of title 5, United States Code (commonly known as the "Federal Vacancies Reform Act of 1998").

TITLE II—INFORMATION ANALYSIS

SUBTITLE A—INFORMATION AND ANALYSIS; ACCESS TO INFORMATION

INFORMATION AND ANALYSIS

SEC. 201. [6 U.S.C. § 121]

(a) INTELLIGENCE AND ANALYSIS.—There shall be in the Department an Office of Intelligence and Analysis.

(b) UNDER SECRETARY FOR INTELLIGENCE AND ANALYSIS.—

(1) OFFICE OF INTELLIGENCE AND ANALYSIS.—The Office of Intelligence and Analysis shall be headed by an Under Secretary for Intelligence and Analysis, who shall be appointed by the President, by and with the advice and consent of the Senate.

(2) CHIEF INTELLIGENCE OFFICER.—The Under Secretary for Intelligence and Analysis shall serve as the Chief Intelligence Officer of the Department.

(c) DISCHARGE OF RESPONSIBILITIES.—The Secretary shall ensure that the responsibilities of the Department relating to information analysis and infrastructure protection, including those described in subsection (d), are carried out through the Under Secretary for Intelligence and Analysis.

(d) RESPONSIBILITIES OF SECRETARY RELATING TO INTELLIGENCE AND ANALYSIS.—The responsibilities of the Secretary relating to intelligence and analysis shall be as follows:

(1) To access, receive, and analyze law enforcement information, intelligence information, and other information from agencies of the Federal Government, State and local government agencies (including law enforcement agencies), and private sector entities, and to integrate such information, in support of the mission responsibilities of the Department and the functions of the National Counterterrorism Center established under section 119 of the National Security Act of 1947 (50 U.S.C. [3056]), in order to—

(A) identify and assess the nature and scope of terrorist threats to the homeland;

(B) detect and identify threats of terrorism against the United States; and

(C) understand such threats in light of actual and potential vulnerabilities of the homeland.

(2) To carry out comprehensive assessments of the vulnerabilities of the key resources and critical infrastructure of the United States, including the performance of risk assessments to determine the risks posed by

particular types of terrorist attacks within the United States (including an assessment of the probability of success of such attacks and the feasibility and potential efficacy of various countermeasures to such attacks).

(3) To integrate relevant information, analysis, and vulnerability assessments (regardless of whether such information, analysis or assessments are provided by or produced by the Department) in order to—

(A) identify priorities for protective and support measures regarding terrorist and other threats to homeland security by the Department, other agencies of the Federal Government, State, and local government agencies and authorities, the private sector, and other entities; and

(B) prepare finished intelligence and information products in both classified and unclassified formats, as appropriate, whenever reasonably expected to be of benefit to a State, local, or tribal government (including a State, local, or tribal law enforcement agency) or a private sector entity.

(4) To ensure, pursuant to section 202, the timely and efficient access by the Department to all information necessary to discharge the responsibilities under this section, including obtaining such information from other agencies of the Federal Government.

(5) To review, analyze, and make recommendations for improvements to the policies and procedures governing the sharing of information within the scope of the information sharing environment established under section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (6 U.S.C. 485), including homeland security information, terrorism information, and weapons of mass destruction information, and any policies, guidelines, procedures, instructions, or standards established under that section.

(6) To disseminate, as appropriate, information analyzed by the Department within the Department, to other agencies of the Federal Government with responsibilities relating to homeland security, and to agencies of State and local governments and private sector entities with such responsibilities in order to assist in the deterrence, prevention, preemption of, or response to, terrorist attacks against the United States.

(7) To consult with the Director of National Intelligence and other appropriate intelligence, law enforcement, or other elements of the Federal Government to establish collection priorities and strategies for information, including law enforcement-related information, relating to threats of terrorism against the United States through such means as the

representation of the Department in discussions regarding requirements and priorities in the collection of such information.

(8) To consult with State and local governments and private sector entities to ensure appropriate exchanges of information, including law enforcement-related information, relating to threats of terrorism against the United States.

(9) To ensure that—

(A) any material received pursuant to this Act is protected from unauthorized disclosure and handled and used only for the performance of official duties; and

(B) any intelligence information under this Act is shared, retained, and disseminated consistent with the authority of the Director of National Intelligence to protect intelligence sources and methods under the National Security Act of 1947 and related procedures and, as appropriate, similar authorities of the Attorney General concerning sensitive law enforcement information.

(10) To request additional information from other agencies of the Federal Government, State and local government agencies, and the private sector relating to threats of terrorism in the United States, or relating to other areas of responsibility assigned by the Secretary, including the entry into cooperative agreements through the Secretary to obtain such information.

(11) To establish and utilize, in conjunction with the chief information officer of the Department, a secure communications and information technology infrastructure, including data-mining and other advanced analytical tools, in order to access, receive, and analyze data and information in furtherance of the responsibilities under this section, and to disseminate information acquired and analyzed by the Department, as appropriate.

(12) To ensure, in conjunction with the chief information officer of the Department, that any information databases and analytical tools developed or utilized by the Department—

(A) are compatible with one another and with relevant information databases of other agencies of the Federal Government; and

(B) treat information in such databases in a manner that complies with applicable Federal law on privacy.

(13) To coordinate training and other support to the elements and personnel of the Department, other agencies of the Federal Government, and State and local governments that provide information to the Department, or are consumers of information provided by the

- Department, in order to facilitate the identification and sharing of information revealed in their ordinary duties and the optimal utilization of information received from the Department.
- (14) To coordinate with elements of the intelligence community and with Federal, State, and local law enforcement agencies, and the private sector, as appropriate.
- (15) To provide intelligence and information analysis and support to other elements of the Department.
- (16) To coordinate and enhance integration among the intelligence components of the Department, including through strategic oversight of the intelligence activities of such components.
- (17) To establish the intelligence collection, processing, analysis, and dissemination priorities, policies, processes, standards, guidelines, and procedures for the intelligence components of the Department, consistent with any directions from the President and, as applicable, the Director of National Intelligence.
- (18) To establish a structure and process to support the missions and goals of the intelligence components of the Department.
- (19) To ensure that, whenever possible, the Department—
- (A) produces and disseminates unclassified reports and analytic products based on open-source information; and
 - (B) produces and disseminates such reports and analytic products contemporaneously with reports or analytic products concerning the same or similar information that the Department produced and disseminated in a classified format.
- (20) To establish within the Office of Intelligence and Analysis an internal continuity of operations plan.
- (21) Based on intelligence priorities set by the President, and guidance from the Secretary and, as appropriate, the Director of National Intelligence—
- (A) to provide to the heads of each intelligence component of the Department guidance for developing the budget pertaining to the activities of such component; and
 - (B) to present to the Secretary a recommendation for a consolidated budget for the intelligence components of the Department, together with any comments from the heads of such components.
- (22) To perform such other duties relating to such responsibilities as the Secretary may provide.
- (23)(A) Not later than six months after the date of the enactment of this paragraph, to conduct an intelligence-based review and comparison of

the risks and consequences of EMP and GMD facing critical infrastructure, and submit to the Committee on Homeland Security and the Permanent Select Committee on Intelligence of the House of Representatives and the Committee on Homeland Security and Governmental Affairs and the Select Committee on Intelligence of the Senate—

- (i) a recommended strategy to protect and prepare the critical infrastructure of the homeland against threats of EMP and GMD; and
- (ii) not less frequently than every two years thereafter for the next six years, updates of the recommended strategy.

- (B) The recommended strategy under subparagraph (A) shall—
- (i) be based on findings of the research and development conducted under section 320;
 - (ii) be developed in consultation with the relevant Federal sector-specific agencies (as defined under Presidential Policy Directive-21) for critical infrastructure;
 - (iii) be developed in consultation with the relevant sector coordinating councils for critical infrastructure;
 - (iv) be informed, to the extent practicable, by the findings of the intelligence-based review and comparison of the risks and consequences of EMP and GMD facing critical infrastructure conducted under subparagraph (A); and
 - (v) be submitted in unclassified form, but may include a classified annex.

(C) The Secretary may, if appropriate, incorporate the recommended strategy into a broader recommendation developed by the Department to help protect and prepare critical infrastructure from terrorism, cyber attacks, and other threats if, as incorporated, the recommended strategy complies with subparagraph (B).

(e) STAFF.—

(1) IN GENERAL.—The Secretary shall provide the Office of Intelligence and Analysis with a staff of analysts having appropriate expertise and experience to assist such offices in discharging responsibilities under this section.

(2) PRIVATE SECTOR ANALYSTS.—Analysts under this subsection may include analysts from the private sector.

(3) SECURITY CLEARANCES.—Analysts under this subsection shall possess security clearances appropriate for their work under this section.

(f) DETAIL OF PERSONNEL.—

(1) IN GENERAL.—In order to assist the Office of Intelligence and Analysis in discharging responsibilities under this section, personnel of the agencies referred to in paragraph (2) may be detailed to the Department for the performance of analytic functions and related duties.

(2) COVERED AGENCIES.—The agencies referred to in this paragraph are as follows:

- (A) The Department of State.
- (B) The Central Intelligence Agency.
- (C) The Federal Bureau of Investigation.
- (D) The National Security Agency.
- (E) The National Geospatial-Intelligence Agency.
- (F) The Defense Intelligence Agency.
- (G) Any other agency of the Federal Government that the President considers appropriate.

(3) COOPERATIVE AGREEMENTS.—The Secretary and the head of the agency concerned may enter into cooperative agreements for the purpose of detailing personnel under this subsection.

(4) BASIS.—The detail of personnel under this subsection may be on a reimbursable or non-reimbursable basis.

(g) FUNCTIONS TRANSFERRED.—In accordance with title XV, there shall be transferred to the Secretary, for assignment to the Office of Intelligence and Analysis and the Office of Infrastructure Protection under this section, the functions, personnel, assets, and liabilities of the following:

- (1) The National Infrastructure Protection Center of the Federal Bureau of Investigation (other than the Computer Investigations and Operations Section), including the functions of the Attorney General relating thereto.
- (2) The National Communications System of the Department of Defense, including the functions of the Secretary of Defense relating thereto.
- (3) The Critical Infrastructure Assurance Office of the Department of Commerce, including the functions of the Secretary of Commerce relating thereto.
- (4) The National Infrastructure Simulation and Analysis Center of the Department of Energy and the energy security and assurance program and activities of the Department, including the functions of the Secretary of Energy relating thereto.
- (5) The Federal Computer Incident Response Center of the General Services Administration, including the functions of the Administrator of General Services relating thereto.

ACCESS TO INFORMATION

SEC. 202. [6 U.S.C. § 122]

(a) IN GENERAL.—

(1) **THREAT AND VULNERABILITY INFORMATION.**—Except as otherwise directed by the President, the Secretary shall have such access as the Secretary considers necessary to all information, including reports, assessments, analyses, and unevaluated intelligence relating to threats of terrorism against the United States and to other areas of responsibility assigned by the Secretary, and to all information concerning infrastructure or other vulnerabilities of the United States to terrorism, whether or not such information has been analyzed, that may be collected, possessed, or prepared by any agency of the Federal Government.

(2) **OTHER INFORMATION.**—The Secretary shall also have access to other information relating to matters under the responsibility of the Secretary that may be collected, possessed, or prepared by an agency of the Federal Government as the President may further provide.

(b) **MANNER OF ACCESS.**—Except as otherwise directed by the President, with respect to information to which the Secretary has access pursuant to this section—

(1) the Secretary may obtain such material upon request, and may enter into cooperative arrangements with other executive agencies to provide such material or provide Department officials with access to it on a regular or routine basis, including requests or arrangements involving broad categories of material, access to electronic databases, or both; and
(2) regardless of whether the Secretary has made any request or entered into any cooperative arrangement pursuant to paragraph (1), all agencies of the Federal Government shall promptly provide to the Secretary—

(A) all reports (including information reports containing intelligence which has not been fully evaluated), assessments, and analytical information relating to threats of terrorism against the United States and to other areas of responsibility assigned by the Secretary;

(B) all information concerning the vulnerability of the infrastructure of the United States, or other vulnerabilities of the United States, to terrorism, whether or not such information has been analyzed;

(C) all other information relating to significant and credible threats of terrorism against the United States, whether or not such information has been analyzed; and

(D) such other information or material as the President may direct.

(c) TREATMENT UNDER CERTAIN LAWS.—The Secretary shall be deemed to be a Federal law enforcement, intelligence, protective, national defense, immigration, or national security official, and shall be provided with all information from law enforcement agencies that is required to be given to the Director of National Intelligence, under any provision of the following:

- (1) The USA PATRIOT Act of 2001(Public Law 107-56).
- (2) Section 2517(6) of title 18, United States Code.
- (3) Rule 6(e)(3)(C) of the Federal Rules of Criminal Procedure.

(d) ACCESS TO INTELLIGENCE AND OTHER INFORMATION.—

(1) ACCESS BY ELEMENTS OF FEDERAL GOVERNMENT.—Nothing in this title shall preclude any element of the intelligence community (as that term is defined in section 3(4) of the National Security Act of 1947 (50 U.S.C. [3003(4)]), or any other element of the Federal Government with responsibility for analyzing terrorist threat information, from receiving any intelligence or other information relating to terrorism.

(2) SHARING OF INFORMATION.—The Secretary, in consultation with the Director of National Intelligence, shall work to ensure that intelligence or other information relating to terrorism to which the Department has access is appropriately shared with the elements of the Federal Government referred to in paragraph (1), as well as with State and local governments, as appropriate.

HOMELAND SECURITY ADVISORY SYSTEM

SEC. 203. [6 U.S.C. § 124]

(a) REQUIREMENT.—The Secretary shall administer the Homeland Security Advisory System in accordance with this section to provide advisories or warnings regarding the threat or risk that acts of terrorism will be committed on the homeland to Federal, State, local, and tribal government authorities and to the people of the United States, as appropriate. The Secretary shall exercise primary responsibility for providing such advisories or warnings.

(b) REQUIRED ELEMENTS.—In administering the Homeland Security Advisory System, the Secretary shall—

- (1) establish criteria for the issuance and revocation of such advisories or warnings;
- (2) develop a methodology, relying on the criteria established under paragraph (1), for the issuance and revocation of such advisories or warnings;

- (3) provide, in each such advisory or warning, specific information and advice regarding appropriate protective measures and countermeasures that may be taken in response to the threat or risk, at the maximum level of detail practicable to enable individuals, government entities, emergency response providers, and the private sector to act appropriately;
- (4) whenever possible, limit the scope of each such advisory or warning to a specific region, locality, or economic sector believed to be under threat or at risk; and
- (5) not, in issuing any advisory or warning, use color designations as the exclusive means of specifying homeland security threat conditions that are the subject of the advisory or warning.

HOMELAND SECURITY INFORMATION SHARING

SEC. 204. [6 U.S.C. § 124a]

- (a) **INFORMATION SHARING.**—Consistent with section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (6 U.S.C. 485), the Secretary, acting through the Under Secretary for Intelligence and Analysis, shall integrate the information and standardize the format of the products of the intelligence components of the Department containing homeland security information, terrorism information, weapons of mass destruction information, or national intelligence (as defined in section 3(5) of the National Security Act of 1947 (50 U.S.C. [3003(5)]) except for any internal security protocols or personnel information of such intelligence components, or other administrative processes that are administered by any chief security officer of the Department.
- (b) **INFORMATION SHARING AND KNOWLEDGE MANAGEMENT OFFICERS.**—For each intelligence component of the Department, the Secretary shall designate an information sharing and knowledge management officer who shall report to the Under Secretary for Intelligence and Analysis regarding coordinating the different systems used in the Department to gather and disseminate homeland security information or national intelligence (as defined in section 3(5) of the National Security Act of 1947 (50 U.S.C. [3003(5)]).
- (c) **STATE, LOCAL, AND PRIVATE-SECTOR SOURCES OF INFORMATION.**—
 - (1) **ESTABLISHMENT OF BUSINESS PROCESSES.**—The Secretary, acting through the Under Secretary for Intelligence and Analysis or the Assistant Secretary for Infrastructure Protection, as appropriate, shall—
 - (A) establish Department-wide procedures for the review and analysis of information provided by State, local, and tribal governments and the private sector;

(B) as appropriate, integrate such information into the information gathered by the Department and other departments and agencies of the Federal Government; and

(C) make available such information, as appropriate, within the Department and to other departments and agencies of the Federal Government.

(2) FEEDBACK.—The Secretary shall develop mechanisms to provide feedback regarding the analysis and utility of information provided by any entity of State, local, or tribal government or the private sector that provides such information to the Department.

(d) TRAINING AND EVALUATION OF EMPLOYEES.—

(1) TRAINING.—The Secretary, acting through the Under Secretary for Intelligence and Analysis or the Director of the Cybersecurity and Infrastructure Security Agency, as appropriate, shall provide to employees of the Department opportunities for training and education to develop an understanding of—

(A) the definitions of homeland security information and national intelligence (as defined in section 3(5) of the National Security Act of 1947 (50 U.S.C. [3003(5)]); and

(B) how information available to such employees as part of their duties—

(i) might qualify as homeland security information or national intelligence; and

(ii) might be relevant to the Office of Intelligence and Analysis and the intelligence components of the Department.

(2) EVALUATIONS.—The Under Secretary for Intelligence and Analysis shall—

(A) on an ongoing basis, evaluate how employees of the Office of Intelligence and Analysis and the intelligence components of the Department are utilizing homeland security information or national intelligence, sharing information within the Department, as described in this title, and participating in the information sharing environment established under section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (6 U.S.C. 485); and

(B) provide to the appropriate component heads regular reports regarding the evaluations under subparagraph (A).

COMPREHENSIVE INFORMATION TECHNOLOGY NETWORK ARCHITECTURE

SEC. 205. [6 U.S.C. § 124b]

(a) **ESTABLISHMENT.**—The Secretary, acting through the Under Secretary for Intelligence and Analysis, shall establish, consistent with the policies and procedures developed under section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (6 U.S.C. 485), and consistent with the enterprise architecture of the Department, a comprehensive information technology network architecture for the Office of Intelligence and Analysis that connects the various databases and related information technology assets of the Office of Intelligence and Analysis and the intelligence components of the Department in order to promote internal information sharing among the intelligence and other personnel of the Department.

(b) **COMPREHENSIVE INFORMATION TECHNOLOGY NETWORK ARCHITECTURE DEFINED.**—The term “comprehensive information technology network architecture” means an integrated framework for evolving or maintaining existing information technology and acquiring new information technology to achieve the strategic management and information resources management goals of the Office of Intelligence and Analysis.

COORDINATION WITH INFORMATION SHARING ENVIRONMENT

SEC. 206. [6 U.S.C. § 124c]

(a) **GUIDANCE.**—All activities to comply with sections 203, 204, and 205 shall be—

- (1) consistent with any policies, guidelines, procedures, instructions, or standards established under section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (6 U.S.C. 485);
- (2) implemented in coordination with, as appropriate, the program manager for the information sharing environment established under that section;
- (3) consistent with any applicable guidance issued by the Director of National Intelligence; and
- (4) consistent with any applicable guidance issued by the Secretary relating to the protection of law enforcement information or proprietary information.

(b) **CONSULTATION.**—In carrying out the duties and responsibilities under this subtitle, the Under Secretary for Intelligence and Analysis shall take into account the views of the heads of the intelligence components of the Department.

INTELLIGENCE COMPONENTS

SEC. 207. [6 U.S.C. § 124d]

Subject to the direction and control of the Secretary, and consistent with any applicable guidance issued by the Director of National Intelligence, the responsibilities of the head of each intelligence component of the Department are as follows:

- (1) To ensure that the collection, processing, analysis, and dissemination of information within the scope of the information sharing environment, including homeland security information, terrorism information, weapons of mass destruction information, and national intelligence (as defined in section 3(5) of the National Security Act of 1947 (50 U.S.C. [3003(5)]), are carried out effectively and efficiently in support of the intelligence mission of the Department, as led by the Under Secretary for Intelligence and Analysis.
- (2) To otherwise support and implement the intelligence mission of the Department, as led by the Under Secretary for Intelligence and Analysis.
- (3) To incorporate the input of the Under Secretary for Intelligence and Analysis with respect to performance appraisals, bonus or award recommendations, pay adjustments, and other forms of commendation.
- (4) To coordinate with the Under Secretary for Intelligence and Analysis in developing policies and requirements for the recruitment and selection of intelligence officials of the intelligence component.
- (5) To advise and coordinate with the Under Secretary for Intelligence and Analysis on any plan to reorganize or restructure the intelligence component that would, if implemented, result in realignments of intelligence functions.
- (6) To ensure that employees of the intelligence component have knowledge of, and comply with, the programs and policies established by the Under Secretary for Intelligence and Analysis and other appropriate officials of the Department and that such employees comply with all applicable laws and regulations.
- (7) To perform such other activities relating to such responsibilities as the Secretary may provide.

TRAINING FOR EMPLOYEES OF INTELLIGENCE COMPONENTS

SEC. 208. [6 U.S.C. § 124e]

The Secretary shall provide training and guidance for employees, officials, and senior executives of the intelligence components of the Department to develop knowledge of laws, regulations, operations, policies, procedures, and programs

that are related to the functions of the Department relating to the collection, processing, analysis, and dissemination of information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information, or national intelligence (as defined in section 3(5) of the National Security Act of 1947 (50 U.S.C. [3003(5)]).

**INTELLIGENCE TRAINING DEVELOPMENT FOR STATE AND LOCAL
GOVERNMENT OFFICIALS**

SEC. 209. [6 U.S.C. § 124f]

(a) CURRICULUM.—The Secretary, acting through the Under Secretary for Intelligence and Analysis, shall—

(1) develop a curriculum for training State, local, and tribal government officials, including law enforcement officers, intelligence analysts, and other emergency response providers, in the intelligence cycle and Federal laws, practices, and regulations regarding the development, handling, and review of intelligence and other information; and

(2) ensure that the curriculum includes executive level training for senior level State, local, and tribal law enforcement officers, intelligence analysts, and other emergency response providers.

(b) TRAINING.—To the extent possible, the Federal Law Enforcement Training Center and other existing Federal entities with the capacity and expertise to train State, local, and tribal government officials based on the curriculum developed under subsection (a) shall be used to carry out the training programs created under this section. If such entities do not have the capacity, resources, or capabilities to conduct such training, the Secretary may approve another entity to conduct such training.

(c) CONSULTATION.—In carrying out the duties described in subsection (a), the Under Secretary for Intelligence and Analysis shall consult with the Director of the Federal Law Enforcement Training Center, the Attorney General, the Director of National Intelligence, the Administrator of the Federal Emergency Management Agency, and other appropriate parties, such as private industry, institutions of higher education, nonprofit institutions, and other intelligence agencies of the Federal Government.

INFORMATION SHARING INCENTIVES

SEC. 210. [6 U.S.C. § 124g]

(a) AWARDS.—In making cash awards under chapter 45 of title 5, United States Code, the President or the head of an agency, in consultation with the program

manager designated under section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (6 U.S.C. 485), may consider the success of an employee in appropriately sharing information within the scope of the information sharing environment established under that section, including homeland security information, terrorism information, and weapons of mass destruction information, or national intelligence (as defined in section 3(5) of the National Security Act of 1947 (50 U.S.C. [3003(5)]), in a manner consistent with any policies, guidelines, procedures, instructions, or standards established by the President or, as appropriate, the program manager of that environment for the implementation and management of that environment.

(b) OTHER INCENTIVES.—The head of each department or agency described in section 1016h of the Intelligence Reform and Terrorism Prevention Act of 2004, in consultation with the program manager designated under section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (6 U.S.C. 485), shall adopt best practices regarding effective ways to educate and motivate officers and employees of the Federal Government to participate fully in the information sharing environment, including—

- (1) promotions and other nonmonetary awards; and
- (2) publicizing information sharing accomplishments by individual employees and, where appropriate, the tangible end benefits that resulted.

**DEPARTMENT OF HOMELAND SECURITY STATE, LOCAL,
AND REGIONAL FUSION CENTER INITIATIVE**

SEC. 210A. [6 U.S.C. § 124H]

(a) ESTABLISHMENT.—The Secretary, in consultation with the program manager of the information sharing environment established under section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (6 U.S.C. 485), the Attorney General, the Privacy Officer of the Department, the Officer for Civil Rights and Civil Liberties of the Department, and the Privacy and Civil Liberties Oversight Board established under section 1061 of the Intelligence Reform and Terrorism Prevention Act of 2004 (5 U.S.C. 601 note), shall establish a Department of Homeland Security State, Local, and Regional Fusion Center Initiative to establish partnerships with State, local, and regional fusion centers.

(b) DEPARTMENT SUPPORT AND COORDINATION.—Through the Department of Homeland Security State, Local, and Regional Fusion Center Initiative, and in coordination with the principal officials of participating State, local, or regional fusion centers and the officers designated as the Homeland Security Advisors of the States, the Secretary shall—

- (1) provide operational and intelligence advice and assistance to State, local, and regional fusion centers;

- (2) support efforts to include State, local, and regional fusion centers into efforts to establish an information sharing environment;
- (3) conduct tabletop and live training exercises to regularly assess the capability of individual and regional networks of State, local, and regional fusion centers to integrate the efforts of such networks with the efforts of the Department;
- (4) coordinate with other relevant Federal entities engaged in homeland security-related activities;
- (5) provide analytic and reporting advice and assistance to State, local, and regional fusion centers;
- (6) review information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information, that is gathered by State, local, and regional fusion centers, and to incorporate such information, as appropriate, into the Department's own such information;
- (7) provide management assistance to State, local, and regional fusion centers;
- (8) serve as a point of contact to ensure the dissemination of information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information;
- (9) facilitate close communication and coordination between State, local, and regional fusion centers and the Department;
- (10) provide State, local, and regional fusion centers with expertise on Department resources and operations;
- (11) provide training to State, local, and regional fusion centers and encourage such fusion centers to participate in terrorism threat-related exercises conducted by the Department; and
- (12) carry out such other duties as the Secretary determines are appropriate.

(c) PERSONNEL ASSIGNMENT.—

- (1) IN GENERAL.—The Under Secretary for Intelligence and Analysis shall, to the maximum extent practicable, assign officers and intelligence analysts from components of the Department to participating State, local, and regional fusion centers.
- (2) PERSONNEL SOURCES.—Officers and intelligence analysts assigned to participating fusion centers under this subsection may be assigned from the following Department components, in coordination with the respective component head and in consultation with the principal officials of participating fusion centers:

- (A) Office of Intelligence and Analysis.
- (B) Cybersecurity and Infrastructure Security Agency.
- (C) Transportation Security Administration.
- (D) United States Customs and Border Protection.
- (E) United States Immigration and Customs Enforcement.
- (F) United States Coast Guard.
- (G) Other components of the Department, as determined by the Secretary.

(3) QUALIFYING CRITERIA—

(A) IN GENERAL.—The Secretary shall develop qualifying criteria for a fusion center to participate in the assigning of Department officers or intelligence analysts under this section.

(B) CRITERIA.—Any criteria developed under subparagraph (A) may include—

- (i) whether the fusion center, through its mission and governance structure, focuses on a broad counterterrorism approach, and whether that broad approach is pervasive through all levels of the organization;
- (ii) whether the fusion center has sufficient numbers of adequately trained personnel to support a broad counterterrorism mission;
- (iii) whether the fusion center has—
 - (I) access to relevant law enforcement, emergency response, private sector, open source, and national security data; and
 - (II) the ability to share and analytically utilize that data for lawful purposes;
- (iv) whether the fusion center is adequately funded by the State, local, or regional government to support its counterterrorism mission; and
- (v) the relevancy of the mission of the fusion center to the particular source component of Department officers or intelligence analysts.

(4) PREREQUISITE.—

(A) INTELLIGENCE ANALYSIS, PRIVACY, AND CIVIL LIBERTIES TRAINING.—Before being assigned to a fusion center under this section, an officer or intelligence analyst shall undergo—

- (i) appropriate intelligence analysis or information sharing training using an intelligence-led policing curriculum that is consistent with—

- (I) standard training and education programs offered to Department law enforcement and intelligence personnel; and
 - (II) the Criminal Intelligence Systems Operating Policies under part 23 of title 28, Code of Federal Regulations (or any corresponding similar rule or regulation);
 - (ii) appropriate privacy and civil liberties training that is developed, supported, or sponsored by the Privacy Officer appointed under section 222 and the Officer for Civil Rights and Civil Liberties of the Department, in consultation with the Privacy and Civil Liberties Oversight Board established under section 1061 of the Intelligence Reform and Terrorism Prevention Act of 2004 (5 U.S.C. 601 note); and
 - (iii) such other training prescribed by the Under Secretary for Intelligence and Analysis.
- (B) **PRIOR WORK EXPERIENCE IN AREA.**—In determining the eligibility of an officer or intelligence analyst to be assigned to a fusion center under this section, the Under Secretary for Intelligence and Analysis shall consider the familiarity of the officer or intelligence analyst with the State, locality, or region, as determined by such factors as whether the officer or intelligence analyst—
- (i) has been previously assigned in the geographic area; or
 - (ii) has previously worked with intelligence officials or law enforcement or other emergency response providers from that State, locality, or region.
- (5) **EXPEDITED SECURITY CLEARANCE PROCESSING.**—The Under Secretary for Intelligence and Analysis—
- (A) shall ensure that each officer or intelligence analyst assigned to a fusion center under this section has the appropriate security clearance to contribute effectively to the mission of the fusion center; and
 - (B) may request that security clearance processing be expedited for each such officer or intelligence analyst and may use available funds for such purpose.
- (6) **FURTHER QUALIFICATIONS.**—Each officer or intelligence analyst assigned to a fusion center under this section shall satisfy any other

qualifications the Under Secretary for Intelligence and Analysis may prescribe.

(d) **RESPONSIBILITIES.**—An officer or intelligence analyst assigned to a fusion center under this section shall—

- (1) assist law enforcement agencies and other emergency response providers of State, local, and tribal governments and fusion center personnel in using information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information, to develop a comprehensive and accurate threat picture;
- (2) review homeland security-relevant information from law enforcement agencies and other emergency response providers of State, local, and tribal government;
- (3) create intelligence and other information products derived from such information and other homeland security-relevant information provided by the Department; and
- (4) assist in the dissemination of such products, as coordinated by the Under Secretary for Intelligence and Analysis, to law enforcement agencies and other emergency response providers of State, local, and tribal government, other fusion centers, and appropriate Federal agencies.

(e) **BORDER INTELLIGENCE PRIORITY.**—

(1) **IN GENERAL.**—The Secretary shall make it a priority to assign officers and intelligence analysts under this section from United States Customs and Border Protection, United States Immigration and Customs Enforcement, and the Coast Guard to participating State, local, and regional fusion centers located in jurisdictions along land or maritime borders of the United States in order to enhance the integrity of and security at such borders by helping Federal, State, local, and tribal law enforcement authorities to identify, investigate, and otherwise interdict persons, weapons, and related contraband that pose a threat to homeland security.

(2) **BORDER INTELLIGENCE PRODUCTS.**—When performing the responsibilities described in subsection (d), officers and intelligence analysts assigned to participating State, local, and regional fusion centers under this section shall have, as a primary responsibility, the creation of border intelligence products that—

- (A) assist State, local, and tribal law enforcement agencies in deploying their resources most efficiently to help detect and interdict terrorists, weapons of mass destruction, and related contraband at land or maritime borders of the United States;

(B) promote more consistent and timely sharing of border security-relevant information among jurisdictions along land or maritime borders of the United States; and

(C) enhance the Department's situational awareness of the threat of acts of terrorism at or involving the land or maritime borders of the United States.

(f) DATABASE ACCESS.—In order to fulfill the objectives described under subsection (d), each officer or intelligence analyst assigned to a fusion center under this section shall have appropriate access to all relevant Federal databases and information systems, consistent with any policies, guidelines, procedures, instructions, or standards established by the President or, as appropriate, the program manager of the information sharing environment for the implementation and management of that environment.

(g) CONSUMER FEEDBACK.—

(1) IN GENERAL.—The Secretary shall create a voluntary mechanism for any State, local, or tribal law enforcement officer or other emergency response provider who is a consumer of the intelligence or other information products referred to in subsection (d) to provide feedback to the Department on the quality and utility of such intelligence products.

(2) REPORT.—Not later than one year after the date of the enactment of the Implementing Recommendations of the 9/11 Commission Act of 2007, and annually thereafter, the Secretary shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives a report that includes a description of the consumer feedback obtained under paragraph (1) and, if applicable, how the Department has adjusted its production of intelligence products in response to that consumer feedback.

(h) RULE OF CONSTRUCTION.—

(1) IN GENERAL.—The authorities granted under this section shall supplement the authorities granted under section 201(d) and nothing in this section shall be construed to abrogate the authorities granted under section 201(d).

(2) PARTICIPATION.—Nothing in this section shall be construed to require a State, local, or regional government or entity to accept the assignment of officers or intelligence analysts of the Department into the fusion center of that State, locality, or region.

(i) GUIDELINES.—The Secretary, in consultation with the Attorney General, shall establish guidelines for fusion centers created and operated by State and local governments, to include standards that any such fusion center shall—

- (1) collaboratively develop a mission statement, identify expectations and goals, measure performance, and determine effectiveness for that fusion center;
- (2) create a representative governance structure that includes law enforcement officers and other emergency response providers and, as appropriate, the private sector;
- (3) create a collaborative environment for the sharing of intelligence and information among Federal, State, local, and tribal government agencies (including law enforcement officers and other emergency response providers), the private sector, and the public, consistent with any policies, guidelines, procedures, instructions, or standards established by the President or, as appropriate, the program manager of the information sharing environment;
- (4) leverage the databases, systems, and networks available from public and private sector entities, in accordance with all applicable laws, to maximize information sharing;
- (5) develop, publish, and adhere to a privacy and civil liberties policy consistent with Federal, State, and local law;
- (6) provide, in coordination with the Privacy Officer of the Department and the Officer for Civil Rights and Civil Liberties of the Department, appropriate privacy and civil liberties training for all State, local, tribal, and private sector representatives at the fusion center;
- (7) ensure appropriate security measures are in place for the facility, data, and personnel;
- (8) select and train personnel based on the needs, mission, goals, and functions of that fusion center;
- (9) offer a variety of intelligence and information services and products to recipients of fusion center intelligence and information; and
- (10) incorporate law enforcement officers, other emergency response providers, and, as appropriate, the private sector, into all relevant phases of the intelligence and fusion process, consistent with the mission statement developed under paragraph (1), either through full time representatives or liaison relationships with the fusion center to enable the receipt and sharing of information and intelligence.

(j) FUSION CENTER INFORMATION SHARING STRATEGY.—Not later than 1 year after the date of the enactment of the DHS Field Engagement Accountability Act, and not less frequently than once every 5 years thereafter, the Secretary shall develop or update a strategy for Department engagement with fusion centers. Such strategy shall be developed and updated in consultation with heads of intelligence components of the Department, the Chief Privacy Officer, the Officer for Civil Rights and Civil Liberties, officials of fusion centers, officers

designated as Homeland Security Advisors, and the heads of other relevant agencies, as appropriate. Such strategy shall include the following:

(1) Specific goals and objectives for sharing information and engaging with fusion centers—

(A) through the direct deployment of personnel from intelligence components of the Department;

(B) through the use of Department unclassified and classified information sharing systems, including Homeland Security Information network and the Homeland Secure Data Network, or any successor system; and

(C) through any additional means.

(2) The performance metrics to be used to measure success in achieving the goals and objectives referred to in paragraph (1).

(3) A 5-year plan for continued engagement with fusion centers.

(k) DEFINITIONS.—In this section—

(1) the term “fusion center” means a collaborative effort of 2 or more Federal, State, local, or tribal government agencies that combines resources, expertise, or information with the goal of maximizing the ability of such agencies to detect, prevent, investigate, apprehend, and respond to criminal or terrorist activity;

(2) the term “information sharing environment” means the information sharing environment established under section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (6 U.S.C. 485);

(3) the term “intelligence analyst” means an individual who regularly advises, administers, supervises, or performs work in the collection, gathering, analysis, evaluation, reporting, production, or dissemination of information on political, economic, social, cultural, physical, geographical, scientific, or military conditions, trends, or forces in foreign or domestic areas that directly or indirectly affect national security;

(4) the term “intelligence-led policing” means the collection and analysis of information to produce an intelligence end product designed to inform law enforcement decision making at the tactical and strategic levels; and

(5) the term “terrorism information” has the meaning given that term in section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (6 U.S.C. 485).

(l) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to be appropriated \$10,000,000 for each of fiscal years 2008 through 2012, to carry out this section, except for subsection (i), including for hiring officers and intelligence analysts to replace officers and intelligence analysts who are assigned to fusion centers under this section.

HOMELAND SECURITY INFORMATION SHARING FELLOWS PROGRAM

SEC. 210B. [6 U.S.C. § 124i]

(a) ESTABLISHMENT.—

(1) IN GENERAL.—The Secretary, acting through the Under Secretary for Intelligence and Analysis, and in consultation with the Chief Human Capital Officer, shall establish a fellowship program in accordance with this section for the purpose of—

(A) detailing State, local, and tribal law enforcement officers and intelligence analysts to the Department in accordance with subchapter VI of chapter 33 of title 5, United States Code, to participate in the work of the Office of Intelligence and Analysis in order to become familiar with—

(i) the relevant missions and capabilities of the Department and other Federal agencies; and

(ii) the role, programs, products, and personnel of the Office of Intelligence and Analysis; and

(B) promoting information sharing between the Department and State, local, and tribal law enforcement officers and intelligence analysts by assigning such officers and analysts to—

(i) serve as a point of contact in the Department to assist in the representation of State, local, and tribal information requirements;

(ii) identify information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information, that is of interest to State, local, and tribal law enforcement officers, intelligence analysts, and other emergency response providers;

(iii) assist Department analysts in preparing and disseminating products derived from information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information, that are tailored to State, local, and tribal law enforcement officers and intelligence analysts and designed to prepare for and thwart acts of terrorism; and

(iv) assist Department analysts in preparing products derived from information within the scope of the information sharing environment, including homeland

security information, terrorism information, and weapons of mass destruction information, that are tailored to State, local, and tribal emergency response providers and assist in the dissemination of such products through appropriate Department channels.

(2) PROGRAM NAME.—The program under this section shall be known as the “Homeland Security Information Sharing Fellows Program.”

(b) ELIGIBILITY.—

(1) IN GENERAL.—In order to be eligible for selection as an Information Sharing Fellow under the program under this section, an individual shall—

- (A) have homeland security-related responsibilities;
- (B) be eligible for an appropriate security clearance;
- (C) possess a valid need for access to classified information, as determined by the Under Secretary for Intelligence and Analysis;
- (D) be an employee of an eligible entity; and
- (E) have undergone appropriate privacy and civil liberties training that is developed, supported, or sponsored by the Privacy Officer and the Officer for Civil Rights and Civil Liberties, in consultation with the Privacy and Civil Liberties Oversight Board established under section 1061 of the Intelligence Reform and Terrorism Prevention Act of 2004 (5 U.S.C. 601 note).

(2) ELIGIBLE ENTITIES.—In this subsection, the term “eligible entity” means—

- (A) a State, local, or regional fusion center;
- (B) a State or local law enforcement or other government entity that serves a major metropolitan area, suburban area, or rural area, as determined by the Secretary;
- (C) a State or local law enforcement or other government entity with port, border, or agricultural responsibilities, as determined by the Secretary;
- (D) a tribal law enforcement or other authority; or
- (E) such other entity as the Secretary determines is appropriate.

(c) OPTIONAL PARTICIPATION.—No State, local, or tribal law enforcement or other government entity shall be required to participate in the Homeland Security Information Sharing Fellows Program.

(d) PROCEDURES FOR NOMINATION AND SELECTION.—

(1) IN GENERAL.—The Under Secretary for Intelligence and Analysis shall establish procedures to provide for the nomination and selection of

individuals to participate in the Homeland Security Information Sharing Fellows Program.

(2) LIMITATIONS.—The Under Secretary for Intelligence and Analysis shall—

(A) select law enforcement officers and intelligence analysts representing a broad cross-section of State, local, and tribal agencies; and

(B) ensure that the number of Information Sharing Fellows selected does not impede the activities of the Office of Intelligence and Analysis.

CLASSIFIED INFORMATION ADVISORY OFFICER

SEC. 210E. [6 U.S.C. § 124m]

(a) REQUIREMENT TO ESTABLISH.—The Secretary shall identify and designate within the Department a Classified Information Advisory Officer, as described in this section.

(b) RESPONSIBILITIES.—The responsibilities of the Classified Information Advisory Officer shall be as follows:

(1) To develop and disseminate educational materials and to develop and administer training programs to assist state, local, and tribal governments (including state, local, and tribal law enforcement agencies) and private sector entities—

(A) in developing plans and policies to respond to requests related to classified information without communicating such information to individuals who lack appropriate security clearances;

(B) regarding the appropriate procedures for challenging classification designations of information received by personnel of such entities; and

(C) on the means by which such personnel may apply for security clearances.

(2) To inform the Under Secretary for Intelligence and Analysis on policies and procedures that could facilitate the sharing of classified information with such personnel, as appropriate.

(c) INITIAL DESIGNATION.—Not later than 90 days after the date of the enactment of the Reducing Over-Classification Act, the Secretary shall—

(1) designate the initial Classified Information Advisory Officer; and

(2) submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives a written notification of the designation.

TITLE V—NATIONAL EMERGENCY MANAGEMENT

NATIONAL OPERATIONS CENTER

SEC. 515. [6 U.S.C. § 321d]

(a) **DEFINITION.**—In this section, the term “situational awareness” means information gathered from a variety of sources that, when communicated to emergency managers, decision makers, and other appropriate officials, can form the basis for incident management decisionmaking and steady-state activity.

(b) **ESTABLISHMENT.**—The National Operations Center is the principal operations center for the Department and shall—

(1) provide situational awareness and a common operating picture for the entire Federal Government, and for State, local, tribal, and territorial governments, the private sector, and international partners as appropriate, for events, threats, and incidents involving a natural disaster, act of terrorism, or other man-made disaster;

(2) ensure that critical terrorism and disaster-related information reaches government decision-makers; and

(3) enter into agreements with other Federal operations centers and other homeland security partners, as appropriate, to facilitate the sharing of information.

(c) **STATE AND LOCAL EMERGENCY RESPONDER REPRESENTATION.**—

(1) **ESTABLISHMENT OF POSITIONS.**—The Secretary shall establish a position, on a rotating basis, for a representative of State and local emergency responders at the National Operations Center established under subsection (b) to ensure the effective sharing of information between the Federal Government and State and local emergency response services.

(2) **MANAGEMENT.**—The Secretary shall manage the position established pursuant to paragraph (1) in accordance with such rules, regulations, and practices as govern other similar rotating positions at the National Operations Center.

**TITLE VIII—COORDINATION WITH NON-FEDERAL ENTITIES;
INSPECTOR GENERAL; UNITED STATES SECRET SERVICE;
COAST GUARD; GENERAL PROVISIONS**

SUBTITLE A—COORDINATION WITH NON-FEDERAL ENTITIES

OFFICE FOR STATE AND LOCAL GOVERNMENT COORDINATION

SEC. 801. [6 U.S.C. § 361]

(a) **ESTABLISHMENT.**—There is established within the Office of the Secretary the Office for State and Local Government Coordination, to oversee and coordinate departmental programs for and relationships with State and local governments.

(b) **RESPONSIBILITIES.**—The Office established under subsection (a) shall—

- (1) coordinate the activities of the Department relating to State and local government;
- (2) assess, and advocate for, the resources needed by State and local government to implement the national strategy for combating terrorism;
- (3) provide State and local government with regular information, research, and technical support to assist local efforts at securing the homeland; and
- (4) develop a process for receiving meaningful input from State and local government to assist the development of the national strategy for combating terrorism and other homeland security activities.

SUBTITLE I—INFORMATION SHARING

SHORT TITLE; FINDINGS; AND SENSE OF CONGRESS

SEC. 891. [6 U.S.C. § 481]

(a) **SHORT TITLE.**—This subtitle may be cited as the “Homeland Security Information Sharing Act”.

(b) **FINDINGS.**—Congress finds the following:

- (1) The Federal Government is required by the Constitution to provide for the common defense, which includes terrorist attack.
- (2) The Federal Government relies on State and local personnel to protect against terrorist attack.
- (3) The Federal Government collects, creates, manages, and protects classified and sensitive but unclassified information to enhance homeland security.
- (4) Some homeland security information is needed by the State and local personnel to prevent and prepare for terrorist attack.

(5) The needs of State and local personnel to have access to relevant homeland security information to combat terrorism must be reconciled with the need to preserve the protected status of such information and to protect the sources and methods used to acquire such information.

(6) Granting security clearances to certain State and local personnel is one way to facilitate the sharing of information regarding specific terrorist threats among Federal, State, and local levels of government.

(7) Methods exist to declassify, redact, or otherwise adapt classified information so it may be shared with State and local personnel without the need for granting additional security clearances.

(8) State and local personnel have capabilities and opportunities to gather information on suspicious activities and terrorist threats not possessed by Federal agencies.

(9) The Federal Government and State and local governments and agencies in other jurisdictions may benefit from such information.

(10) Federal, State, and local governments and intelligence, law enforcement, and other emergency preparation and response agencies must act in partnership to maximize the benefits of information gathering and analysis to prevent and respond to terrorist attacks.

(11) Information systems, including the National Law Enforcement Telecommunications System and the Terrorist Threat Warning System, have been established for rapid sharing of classified and sensitive but unclassified information among Federal, State, and local entities.

(12) Increased efforts to share homeland security information should avoid duplicating existing information systems.

(c) SENSE OF CONGRESS.—It is the sense of Congress that Federal, State, and local entities should share homeland security information to the maximum extent practicable, with special emphasis on hard-to-reach urban and rural communities.

FACILITATING HOMELAND SECURITY INFORMATION SHARING PROCEDURES

SEC. 892. [6 U.S.C. § 482]

(a) PROCEDURES FOR DETERMINING EXTENT OF SHARING OF HOMELAND SECURITY INFORMATION.—

(1) The President shall prescribe and implement procedures under which relevant Federal agencies—

(A) share relevant and appropriate homeland security information with other Federal agencies, including the Department, and appropriate State and local personnel;

(B) identify and safeguard homeland security information that is sensitive but unclassified; and

(C) to the extent such information is in classified form, determine whether, how, and to what extent to remove classified information, as appropriate, and with which such personnel it may be shared after such information is removed.

(2) The President shall ensure that such procedures apply to all agencies of the Federal Government.

(3) Such procedures shall not change the substantive requirements for the classification and safeguarding of classified information.

(4) Such procedures shall not change the requirements and authorities to protect sources and methods.

(b) PROCEDURES FOR SHARING OF HOMELAND SECURITY INFORMATION.—

(1) Under procedures prescribed by the President, all appropriate agencies, including the intelligence community, shall, through information sharing systems, share homeland security information with Federal agencies and appropriate State and local personnel to the extent such information may be shared, as determined in accordance with subsection(a), together with assessments of the credibility of such information.

(2) Each information sharing system through which information is shared under paragraph(1) shall—

(A) have the capability to transmit unclassified or classified information, though the procedures and recipients for each capability may differ;

(B) have the capability to restrict delivery of information to specified subgroups by geographic location, type of organization, position of a recipient within an organization, or a recipient's need to know such information;

(C) be configured to allow the efficient and effective sharing of information; and

(D) be accessible to appropriate State and local personnel.

(3) The procedures prescribed under paragraph(1) shall establish conditions on the use of information shared under paragraph(1)—

(A) to limit the dissemination of such information to ensure that such information is not used for an unauthorized purpose;

(B) to ensure the security and confidentiality of such information;

(C) to protect the constitutional and statutory rights of any individuals who are subjects of such information; and

(D) to provide data integrity through the timely removal and destruction of obsolete or erroneous names and information.

(4) The procedures prescribed under paragraph(1) shall ensure, to the greatest extent practicable, that the information sharing system through which information is shared under such paragraph include existing information sharing systems, including, but not limited to, the National Law Enforcement Telecommunications System, the Regional Information Sharing System, and the Terrorist Threat Warning System of the Federal Bureau of Investigation.

(5) Each appropriate Federal agency, as determined by the President, shall have access to each information sharing system through which information is shared under paragraph(1), and shall therefore have access to all information, as appropriate, shared under such paragraph.

(6) The procedures prescribed under paragraph(1) shall ensure that appropriate State and local personnel are authorized to use such information sharing systems—

(A) to access information shared with such personnel; and

(B) to share, with others who have access to such information sharing systems, the homeland security information of their own jurisdictions, which shall be marked appropriately as pertaining to potential terrorist activity.

(7) Under procedures prescribed jointly by the Director of Central Intelligence and the Attorney General, each appropriate Federal agency, as determined by the President, shall review and assess the information shared under paragraph(6) and integrate such information with existing intelligence.

(c) SHARING OF CLASSIFIED INFORMATION AND SENSITIVE BUT UNCLASSIFIED INFORMATION WITH STATE AND LOCAL PERSONNEL.—

(1) The President shall prescribe procedures under which Federal agencies may, to the extent the President considers necessary, share with appropriate State and local personnel homeland security information that remains classified or otherwise protected after the determinations prescribed under the procedures set forth in subsection(a).

(2) It is the sense of Congress that such procedures may include 1 or more of the following means:

(A) Carrying out security clearance investigations with respect to appropriate State and local personnel.

(B) With respect to information that is sensitive but unclassified, entering into nondisclosure agreements with appropriate State and local personnel.

(C) Increased use of information-sharing partnerships that include appropriate State and local personnel, such as the Joint Terrorism Task Forces of the Federal Bureau of Investigation,

the Anti-Terrorism Task Forces of the Department of Justice, and regional Terrorism Early Warning Groups.

(3)(A) The Secretary shall establish a program to provide appropriate training to officials described in subparagraph(B) in order to assist such officials in—

- (i) identifying sources of potential terrorist threats through such methods as the Secretary determines appropriate;
- (ii) reporting information relating to such potential terrorist threats to the appropriate Federal agencies in the appropriate form and manner;
- (iii) assuring that all reported information is systematically submitted to and passed on by the Department for use by appropriate Federal agencies; and
- (iv) understanding the mission and roles of the intelligence community to promote more effective information sharing among Federal, State, and local officials and representatives of the private sector to prevent terrorist attacks against the United States.

(B) The officials referred to in subparagraph (A) are officials of State and local government agencies and representatives of private sector entities with responsibilities relating to the oversight and management of first responders, counterterrorism activities, or critical infrastructure.

(C) The Secretary shall consult with the Attorney General to ensure that the training program established in subparagraph (A) does not duplicate the training program established in section 908 of the USA PATRIOT Act (Public Law 107-56; 28 U.S.C. 509 note).

(D) The Secretary shall carry out this paragraph in consultation with the Director of Central Intelligence and the Attorney General.

(d) RESPONSIBLE OFFICIALS.—For each affected Federal agency, the head of such agency shall designate an official to administer this Act with respect to such agency.

(e) FEDERAL CONTROL OF INFORMATION.—Under procedures prescribed under this section, information obtained by a State or local government from a Federal agency under this section shall remain under the control of the Federal agency, and a State or local law authorizing or requiring such a government to disclose information shall not apply to such information.

(f) DEFINITIONS.—As used in this section:

- (1) The term “homeland security information” means any information possessed by a Federal, State, or local agency that—
- (A) relates to the threat of terrorist activity;
 - (B) relates to the ability to prevent, interdict, or disrupt terrorist activity;
 - (C) would improve the identification or investigation of a suspected terrorist or terrorist organization; or
 - (D) would improve the response to a terrorist act.
- (2) The term “intelligence community” has the meaning given such term in section 3(4) of the National Security Act of 1947(50 U.S.C. [3003(4)]).
- (3) The term “State and local personnel” means any of the following persons involved in prevention, preparation, or response for terrorist attack:
- (A) State Governors, mayors, and other locally elected officials.
 - (B) State and local law enforcement personnel and firefighters.
 - (C) Public health and medical professionals.
 - (D) Regional, State, and local emergency management agency personnel, including State adjutant generals.
 - (E) Other appropriate emergency response agency personnel.
 - (F) Employees of private-sector entities that affect critical infrastructure, cyber, economic, or public health security, as designated by the Federal Government in procedures developed pursuant to this section.
- (4) The term “State” includes the District of Columbia and any commonwealth, territory, or possession of the United States.
- (g) CONSTRUCTION.—Nothing in this Act shall be construed as authorizing any department, bureau, agency, officer, or employee of the Federal Government to request, receive, or transmit to any other Government entity or personnel, or transmit to any State or local entity or personnel otherwise authorized by this Act to receive homeland security information, any information collected by the Federal Government solely for statistical purposes in violation of any other provision of law relating to the confidentiality of such information.

REPORT

SEC. 893. [6 U.S.C. § 483]

(a) REPORT REQUIRED.—Not later than 12 months after the date of the enactment of this Act, the President shall submit to the congressional committees specified in subsection(b) a report on the implementation of section 892. The report shall include any recommendations for additional measures or appropriation requests,

beyond the requirements of section 892, to increase the effectiveness of sharing of information between and among Federal, State, and local entities.

(b) SPECIFIED CONGRESSIONAL COMMITTEES.—The congressional committees referred to in subsection(a) are the following committees:

- (1) The Permanent Select Committee on Intelligence and the Committee on the Judiciary of the House of Representatives.
- (2) The Select Committee on Intelligence and the Committee on the Judiciary of the Senate.

AUTHORIZATION OF APPROPRIATIONS

SEC. 894. [6 U.S.C. § 484]

There are authorized to be appropriated such sums as may be necessary to carry out section 892.

TITLE XIII—FEDERAL WORKFORCE IMPROVEMENT

SUBTITLE D – ACADEMIC TRAINING

INTELLIGENCE AND CYBERSECURITY DIVERSITY FELLOWSHIP PROGRAM

SEC. 1333. [6 U.S.C. § 665a]

(a) DEFINITIONS.—In this section:

(1) APPROPRIATE COMMITTEES OF CONGRESS.—The term ‘appropriate committees of Congress’ means—

(A) the Committee on Homeland Security and Governmental Affairs and the Select Committee on Intelligence of the Senate; and

(B) the Committee on Homeland Security and the Permanent Select Committee on Intelligence of the House of Representatives.

(2) EXCEPTED SERVICE.—The term ‘excepted service’ has the meaning given that term in section 2103 of title 5, United States Code.

(3) HISTORICALLY BLACK COLLEGE OR UNIVERSITY.—The term ‘historically Black college or university’ has the meaning given the term ‘part B institution’ in section 322 of the Higher Education Act of 1965 (20 U.S.C. 1061).

(4) INSTITUTION OF HIGHER EDUCATION.—The term ‘institution of higher education’ has the meaning given that term in section 101 of the Higher Education Act of 1965 (20 U.S.C. 1001).

(5) **MINORITY-SERVING INSTITUTION.**—The term ‘minority-serving institution’ means an institution of higher education described in section 371(a) of the Higher Education Act of 1965 (20 U.S.C. 1067q(a)).

(b) **PROGRAM.**—The Secretary shall carry out an intelligence and cybersecurity diversity fellowship program (in this section referred to as the ‘Program’) under which an eligible individual may—

(1) participate in a paid internship at the Department that relates to intelligence, cybersecurity, or some combination thereof;

(2) receive tuition assistance from the Secretary; and

(3) upon graduation from an institution of higher education and successful completion of the Program (as defined by the Secretary), receive an offer of employment to work in an intelligence or cybersecurity position of the Department that is in the excepted service.

(c) **ELIGIBILITY.**—To be eligible to participate in the Program, an individual shall—

(1) be a citizen of the United States; and

(2) as of the date of submitting the application to participate in the Program—

(A) have a cumulative grade point average of at least 3.2 on a 4.0 scale;

(B) be a socially disadvantaged individual (as that term is defined in section 124.103 of title 13, Code of Federal Regulations, or successor regulation); and

(C) be a sophomore, junior, or senior at an institution of higher education.

(d) **DIRECT HIRE AUTHORITY.**—If an individual who receives an offer of employment under subsection (b)(3) accepts such offer, the Secretary shall appoint, without regard to provisions of sub-chapter I of chapter 33 of title 5, United States Code, (except for section 3328 of such title) such individual to the position specified in such offer.

(e) **REPORTS.**—

(1) **REPORTS.**—Not later than 1 year after the date of the enactment of this section, and on an annual basis thereafter, the Secretary shall submit to the appropriate committees of Congress a report on the Program.

(2) **MATTERS.**—Each report under paragraph (1) shall include, with respect to the most recent year, the following:

(A) A description of outreach efforts by the Secretary to raise awareness of the Program among institutions of higher education in which eligible individuals are enrolled.

(B) Information on specific recruiting efforts conducted by the Secretary to increase participation in the Program.

(C) The number of individuals participating in the Program, listed by the institution of higher education in which the individual is enrolled at the time of participation, and information on the nature of such participation, including on whether the duties of the individual under the Program relate primarily to intelligence or to cybersecurity.

(D) The number of individuals who accepted an offer of employment under the Program and an identification of the element within the Department to which each individual was appointed.

TITLE XXII—CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

SUBTITLE A – CYBERSECURITY AND INFRASTRUCTURE SECURITY

NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER

SEC. 2209. [6 U.S.C. § 659]

(a) DEFINITIONS.—In this section—

(1) the term ‘cybersecurity purpose’ has the meaning given that term in section 102 of the Cybersecurity Information Sharing Act of 2015 (6 U.S.C. 1501);

(2) the term “‘cybersecurity risk’”—

(A) means threats to and vulnerabilities of information or information systems and any related consequences caused by or resulting from unauthorized access, use, disclosure, degradation, disruption, modification, or destruction of such information or information systems, including such related consequences caused by an act of terrorism; and

(B) does not include any action that solely involves a violation of a consumer term of service or a consumer licensing agreement;

(3) the terms “‘cyber threat indicator’” and “‘defensive measure’” have the meanings given those terms in section 102 of the Cybersecurity Act of 2015;

(4) the term “‘cybersecurity vulnerability’” has the meaning given the term ‘security vulnerability’ in section 102 of the Cybersecurity Information Sharing Act of 2015 (6 U.S.C. 1501);

- (5) the term “incident” means an occurrence that actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information on an information system, or actually or imminently jeopardizes, without lawful authority, an information system;
- (6) the term “information sharing and analysis organization” has the meaning given that term in section 2222(5);
- (7) the term “information system” has the meaning given that term in section 3502(8) of title 44, United States Code;
- (8) the term “security vulnerability” has the meaning given that term in section 102 of the Cybersecurity Information Sharing Act of 2015 (6 U.S.C. 1501); and
- (9) the term “sharing” (including all conjugations thereof) means providing, receiving, and disseminating (including all conjugations of each of such terms).

(b) CENTER.—There is in the Department a national cybersecurity and communications integration center (referred to in this section as the “Center”) to carry out certain responsibilities of the Director. The Center shall be located in the Cybersecurity and Infrastructure Security Agency. The head of the Center shall report to the Assistant Director for Cybersecurity.

(c) FUNCTIONS.—The cybersecurity functions of the Center shall include—

- (1) being a Federal civilian interface for the multi-directional and cross-sector sharing of information related to cyber threat indicators, defensive measures, cybersecurity risks, incidents, analysis, and warnings for Federal and non-Federal entities, including the implementation of title I of the Cybersecurity Act of 2015;
- (2) providing shared situational awareness to enable real time, integrated, and operational actions across the Federal Government and non-Federal entities to address cybersecurity risks and incidents to Federal and non-Federal entities;
- (3) coordinating the sharing of information related to cyber threat indicators, defensive measures, cybersecurity risks, and incidents across the Federal Government;
- (4) facilitating cross-sector coordination to address cybersecurity risks and incidents, including cybersecurity risks and incidents that may be related or could have consequential impacts across multiple sectors;
- (5)(A) conducting integration and analysis, including cross sector integration and analysis, of cyber threat indicators, defensive measures, cybersecurity risks, and incidents; and
 - (B) sharing mitigation protocols to counter cybersecurity vulnerabilities pursuant to subsection (n), as appropriate; and

(C) sharing the analysis conducted under subparagraph (A) and mitigation protocols to counter cybersecurity vulnerabilities in accordance with subparagraph (B), as appropriate, with Federal and non-Federal entities;

(6) upon request, providing timely technical assistance, risk management support, and incident response capabilities to Federal and non-Federal entities with respect to cyber threat indicators, defensive measures, cybersecurity risks, and incidents, which may include attribution, mitigation, and remediation, which may take the form of continuous monitoring and detection of cybersecurity risks to critical infrastructure entities that own or operate industrial control systems that support national critical functions;;

(7) providing information and recommendations on security and resilience measures to Federal and non-Federal entities, including information and recommendations to—

(A) facilitate information security;

(B) strengthen information systems against cybersecurity risks and incidents; and

(C) sharing cyber threat indicators and defensive measures;

(8) engaging with international partners, in consultation with other appropriate agencies, to—

(A) collaborate on cyber threat indicators, defensive measures, and information related to cybersecurity risks and incidents; and

(B) enhance the security and resilience of global cybersecurity;

(9) sharing cyber threat indicators, defensive measures, and other information related to cybersecurity risks and incidents with Federal and non-Federal entities, including across sectors of critical infrastructure and with State and major urban area fusion centers, as appropriate;

(10) participating, as appropriate, in national exercises run by the Department;

(11) in coordination with the Emergency Communications Division of the Department, assessing and evaluating consequence, vulnerability, and threat information regarding cyber incidents to public safety communications to help facilitate continuous improvements to the security and resiliency of such communications; and

(12) detecting, identifying, and receiving information for a cybersecurity purpose about security vulnerabilities relating to critical infrastructure in information systems and devices.

(d) COMPOSITION.—

(1) IN GENERAL.—The Center shall be composed of—

(A) appropriate representatives of Federal entities, such as—

- (i) sector-specific agencies;
 - (ii) civilian and law enforcement agencies; and
 - (iii) elements of the intelligence community, as that term is defined under section 3(4) of the National Security Act of 1947 (50 U.S.C. [3003(4)]);
 - (B) appropriate representatives of non-Federal entities, such as—
 - (i) State, local, and tribal governments;
 - (ii) information sharing and analysis organizations, including information sharing and analysis centers;
 - (iii) owners and operators of critical information systems; and
 - (iv) private entities, including cybersecurity specialists;
 - (C) components within the Center that carry out cybersecurity and communications activities;
 - (D) a designated Federal official for operational coordination with and across each sector;
 - (E) an entity that collaborates with State and local governments on cybersecurity risks and incidents, and has entered into a voluntary information sharing relationship with the Center; and
 - (F) other appropriate representatives or entities, as determined by the Secretary.
- (2) INCIDENTS.—In the event of an incident, during exigent circumstances the Secretary may grant a Federal or non-Federal entity immediate temporary access to the Center.
- (e) PRINCIPLES.—In carrying out the functions under subsection (c), the Center shall ensure—
- (1) to the extent practicable, that—
 - (A) timely, actionable, and relevant cyber threat indicators, defensive measures, and information related to cybersecurity risks, incidents, and analysis is shared;
 - (B) when appropriate, cyber threat indicators, defensive measures, and information related to cybersecurity risks, incidents, and analysis is integrated with other relevant information and tailored to the specific characteristics of a sector;
 - (C) activities are prioritized and conducted based on the level of risk;
 - (D) industry sector-specific, academic, and national laboratory expertise is sought and receives appropriate consideration;
 - (E) continuous, collaborative, and inclusive coordination occurs—

(i) across sectors; and

(ii) with—

(I) sector coordinating councils;

(II) information sharing and analysis organizations;

and

(III) other appropriate non-Federal partners;

(F) as appropriate, the Center works to develop and use mechanisms for sharing information related to cyber threat indicators, defensive measures, cybersecurity risks, and incidents that are technology-neutral, interoperable, real-time, cost-effective, and resilient;

(G) the Center works with other agencies to reduce unnecessarily duplicative sharing of information related to cyber threat indicators, defensive measures, cybersecurity risks, and incidents;

(H) the Center designates an agency contact for non-Federal entities; and

(I) activities of the Center address the security of both information technology and operational technology, including industrial control systems;

(2) that information related to cyber threat indicators, defensive measures, cybersecurity risks, and incidents is appropriately safeguarded against unauthorized access or disclosure; and

(3) that activities conducted by the Center comply with all policies, regulations, and laws that protect the privacy and civil liberties of United States persons, including by working with the Privacy Officer appointed under section 222 to ensure that the Center follows the policies and procedures specified in subsections (b) and (d)(5)(C) of section 105 of the Cybersecurity Act of 2015.

(f) **CYBER HUNT AND INCIDENT RESPONSE TEAMS.**—

(1) **IN GENERAL.**—The Center shall maintain cyber hunt and incident response teams for the purpose of leading Federal asset response activities and providing timely technical assistance to Federal and non-Federal entities, including across all critical infrastructure sectors, regarding actual or potential security incidents, as appropriate and upon request, including—

(A) assistance to asset owners and operators in restoring services following a cyber incident;

(B) identification and analysis of cybersecurity risk and unauthorized cyber activity;

- (C) mitigation strategies to prevent, deter, and protect against cybersecurity risks, and other recommendations, as appropriate;
- (D) recommendations to asset owners and operators for improving overall network and control systems security to lower cybersecurity risks, and other recommendations, as appropriate;
- and
- (E) such other capabilities as the Secretary determines appropriate.

(2) ASSOCIATED METRICS.—The Center Shall—

- (A) define the goals and desired outcomes for each cyber hunt and incident response team; and
- (B) develop metrics—
 - (i) to measure the effectiveness and efficiency of each cyber hunt and incident response team in achieving the goals and desired outcomes defined under subparagraph (A);
 - (ii) that—
 - (I) are quantifiable and actionable; and
 - (II) the center shall use to improve the effectiveness and accountability of, and service delivery by, cyber hunt and incident response.

(3) CYBERSECURITY SPECIALISTS.—After notice to, and with the approval of, the entity requesting action by or technical assistance from the Center, the Secretary may include cybersecurity specialists from the private sector on a cyber hunt and incident response team.

(g) NO RIGHT OR BENEFIT.—

(1) IN GENERAL.—The provision of assistance or information to, and inclusion in the Center or any team or activity of the Center of, governmental or private entities under this section shall be at the sole and unreviewable discretion of the Director.

(2) CERTAIN ASSISTANCE OR INFORMATION.—The provision of certain assistance or information to, or inclusion in the Center or any team or activity of the Center of, one governmental or private entity pursuant to this section shall not create a right or benefit, substantive or procedural, to similar assistance or information for any other governmental or private entity.

(h) AUTOMATED INFORMATION SHARING.—

(1) IN GENERAL.—The Director, in coordination with industry and other stakeholders, shall develop capabilities making use of existing information technology industry standards and best practices, as appropriate, that support and rapidly advance the development, adoption, and implementation of automated mechanisms for the sharing of cyber

threat indicators and defensive measures in accordance with title I of the Cybersecurity Act of 2015.

(2) ANNUAL REPORT.—The Director shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives an annual report on the status and progress of the development of the capabilities described in paragraph (1). Such reports shall be required until such capabilities are fully implemented.

(i) VOLUNTARY INFORMATION SHARING PROCEDURES.—

(1) PROCEDURES.—

(A) IN GENERAL.—The Center may enter into a voluntary information sharing relationship with any consenting non-Federal entity for the sharing of cyber threat poses in accordance with this section. Nothing in this subsection may be construed to require any non-Federal entity to enter into any such information sharing relationship with the Center or any other entity. The Center may terminate a voluntary information sharing relationship under this subsection, at the sole and unreviewable discretion of the Secretary, acting through the Director, for any reason, including if the Center determines that the non-Federal entity with which the Center has entered into such a relationship has violated the terms of this subsection.

(B) NATIONAL SECURITY.—The Secretary may decline to enter into a voluntary information sharing relationship under this subsection, at the sole and unreviewable discretion of the Secretary, acting through the Director, for any reason, including if the Secretary determines that such is appropriate for national security.

(2) VOLUNTARY INFORMATION SHARING RELATIONSHIPS.—A voluntary information sharing relationship under this subsection may be characterized as an agreement described in this paragraph.

(A) STANDARD AGREEMENT.—For the use of a non-Federal entity, the Center shall make available a standard agreement, consistent with this section, on the Department’s website.

(B) NEGOTIATED AGREEMENT.—At the request of a non-Federal entity, and if determined appropriate by the Center, at the sole and unreviewable discretion of the Secretary, acting through the Director, the Department shall negotiate a non-standard agreement, consistent with this section.

(C) EXISTING AGREEMENTS.—An agreement between the Center and a non-Federal entity that is entered into before the date of enactment of this subsection, or such an agreement that is in effect before such date, shall be deemed in compliance with the requirements of this subsection, notwithstanding any other provision or requirements of this subsection. An agreement under this subsection shall include the relevant privacy protections as in effect under the Cooperative Research and Development Agreement for Cybersecurity Information Sharing and Collaboration, as of December 31, 2014. Nothing in this subsection may be construed to require a non-Federal entity to enter into either a standard or negotiated agreement to be in compliance with this subsection.

(j) DIRECT REPORTING.—The Secretary shall develop policies and procedures for direct reporting to the Secretary by the Director of the Center regarding significant cybersecurity risks and incidents.

(k) REPORTS ON INTERNATIONAL COOPERATION.—Not later than 180 days after the date of enactment of this subsection, and periodically thereafter, the Secretary of Homeland Security shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives a report on the range of efforts underway to bolster cybersecurity collaboration with relevant international partners in accordance with subsection (c)(8).

(l) OUTREACH.—Not later than 60 days after the date of enactment of this subsection, the Secretary, acting through the Director, shall—

- (1) disseminate to the public information about how to voluntarily share cyber threat indicators and defensive measures with the Center; and
- (2) enhance outreach to critical infrastructure owners and operators for purposes of such sharing.

(m) CYBERSECURITY OUTREACH.—

(1) IN GENERAL.—The Secretary may leverage small business development centers to provide assistance to small business concerns by disseminating information on cyber threat indicators, defense measures, cybersecurity risks, incidents, analyses, and warnings to help small business concerns in developing or enhancing cybersecurity infrastructure, awareness of cyber threat indicators, and cyber training programs for employees.

(2) DEFINITIONS.—For purposes of this subsection, the terms “small business concern” and “small business development center” have the meaning given such terms, respectively, under section 3 of the Small Business Act.

(n) **COORDINATED VULNERABILITY DISCLOSURE.**—The Secretary, in coordination with industry and other stakeholders, may develop and adhere to Department policies and procedures for coordinating vulnerability disclosures.

(o) **PROTOCOLS TO COUNTER CERTAIN CYBERSECURITY VULNERABILITIES.**—The Director may, as appropriate, identify, develop, and disseminate actionable protocols to mitigate cybersecurity vulnerabilities to information systems and industrial control systems, including in circumstances in which such vulnerabilities exist because software or hardware is no longer supported by a vendor.

(p) **SUBPOENA AUTHORITY.**—

(1) **DEFINITION.**—In this subsection, the term “covered device or system” —

(A) means a device or system commonly used to perform industrial, commercial, scientific, or governmental functions or processes that relate to critical infrastructure, including operational and industrial control systems, distributed control systems, and programmable logic controllers; and

(B) does not include personal devices and systems, such as consumer mobile devices, home computers, residential wireless routers, or residential internet enabled consumer devices.

(2) **AUTHORITY.**—

(A) **In General.**— If the Director identifies a system connected to the internet with a specific security vulnerability and has reason to believe such security vulnerability relates to critical infrastructure and affects a covered device or system, and the Director is unable to identify the entity at risk that owns or operates such covered device or system, the Director may issue a subpoena for the production of information necessary to identify and notify such entity at risk, in order to carry out a function authorized under subsection (c)(12).

(B) **LIMIT ON INFORMATION.**—A subpoena issued pursuant to subparagraph (A) may seek information—

- (i) only in the categories set forth in subparagraph (A), (B), (D), and (E) of section 2703(c)(2) of title 18, United States Code; and
- (ii) for not more than 20 covered devices or systems.

(C) **LIABILITY PROTECTIONS FOR DISCLOSING PROVIDERS.**—The provisions of section 2703(e) of title 18 United States Code, shall apply to any subpoena issued pursuant to subparagraph (A).

(3) **COORDINATION.**—

(A) **IN GENERAL.**— If the Director exercises the subpoena authority under this subsection, and in the interest of avoiding interference with ongoing law enforcement investigations, the Director shall

coordinate the issuance of any such subpoena with the Department of Justice, including the Federal Bureau of Investigation, pursuant to interagency procedures which the Director, in coordination with the Attorney General, shall develop not later than 60 days after the date of the enactment of this subsection.

(B) CONTENTS.—The inter-agency procedures developed under this paragraph shall provide that a subpoena issued by the Director under this subsection shall be—

(i) issued to carry out a function described in subsection (c)(12); and

(ii) subject to the limitations specified in this subsection

(4) NONCOMPLIANCE.— If any person, partnership, corporation, association, or entity fails to comply with any duly served subpoena issued pursuant to this subsection, the Director may request that the Attorney General seek enforcement of such subpoena in any judicial district in which such person, partnership, corporation, association, or entity resides, is found, or transacts business.

(5) NOTICE.— Not later than seven days after the date on which the Director receives information obtained through a subpoena issued pursuant to this subsection, the Director shall notify any entity identified by information obtained pursuant to such subpoena regarding such subpoena and the identified vulnerability.

(6) AUTHENTICATION.—

(A) IN GENERAL.— Any subpoena issued pursuant to this subsection shall be authenticated with a cryptographic digital signature of an authorized representative of the Agency, or other comparable successor technology, that allows the Agency to demonstrate that such subpoena was issued by the Agency and has not been altered or modified since such issuance.

(B) INVALID IF NOT AUTHENTICATED.— Any subpoena issued pursuant to this subsection that is not authenticated in accordance with subparagraph (A) shall not be considered to be valid by the recipient of such subpoena.

(7) PROCEDURES.— Not later than 90 days after the date of the enactment of this subsection, the Director shall establish internal procedures and associated training, applicable to employees and operations of the Agency, regarding subpoenas issued pursuant to this subsection, which shall address the following:

(A) The protection of and restriction on dissemination of nonpublic information obtained through such a subpoena, including a requirement that the Agency not disseminate nonpublic information

obtained through such a subpoena that identifies the party that is subject to such subpoena or the entity at risk identified by information obtained, except that the Agency may share the nonpublic information with the Department of Justice for the purpose of enforcing such subpoena in accordance with paragraph (4), and may share with a Federal agency the nonpublic information of the entity at risk if—

(i) the Agency identifies or is notified of a cybersecurity incident involving such entity, which relates to the vulnerability which led to the issuance of such subpoena;

(ii) the Director determines that sharing the nonpublic information with another Federal department or agency is necessary to allow such department or agency to take a law enforcement or national security action, consistent with the interagency procedures under paragraph (3)(A), or actions related to

(iii) the entity to which the information pertains is notified of the Director's determination, to the extent practicable consistent with national security or law enforcement interests, consistent with such interagency procedures; and

(iv) the entity consents, except that the entity's consent shall not be required if another Federal department or agency identifies the entity to the Agency in connection with a suspected cybersecurity incident.

(B) The restrictions on the use of information obtained through such a subpoena for cybersecurity purpose.

(C) The retention and destruction of nonpublic information obtained through such a subpoena, including—

(i) destruction of such information that the Director determines is unrelated to critical infrastructure immediately upon providing notice to the entity pursuant to paragraph (5); and

(ii) destruction of any personally identifiable information not later than 6 months after the date on which the Director receives information obtained through such a subpoena, unless otherwise agreed to by the individual identified by the subpoena respondent.

(D) The process for providing notice to each party that is subject to such subpoena and each entity identified by information obtained through such subpoena, unless otherwise agreed by the individual identified by the subpoena respondent.

- (E) The processes and criteria for conducting critical infrastructure security risk assessments to determine whether a subpoena is necessary prior to being issued pursuant to this subsection.
- (F) The information to be provided to an entity at risk at the time of the notice of the vulnerability, which shall include—
- (i) a discussion or statement that responding to, or subsequent engagement with, the Agency, is voluntary; and
 - (ii) to the extent practicable, information regarding the process through which the Director identifies security vulnerabilities.
- (8) **LIMITATION ON PROCEDURES.**—The internal procedures established pursuant to paragraph (7) may not require an owner or operator of critical infrastructure to take any action as a result of a notice of vulnerability made pursuant to this Act.
- (9) **REVIEW OF PROCEDURES.**—Not later than 1 year after the date of the enactment of this subsection, the Privacy Officer of the Agency shall—
- (A) review the internal procedures established pursuant to paragraph (7) to ensure that—
 - (i) such procedures are consistent with fair information practices; and
 - (ii) the operations of the Agency comply with such procedures; and
 - (B) notify the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives of the results of the review under subparagraph (A).
- (10) **PUBLICATION OF INFORMATION.**—Not later than 120 days after establishing the internal procedures under paragraph (7) the Director shall publish information on the website of the Agency regarding the subpoena process under this subsection, including information regarding the following:
- (A) Such internal procedures.
 - (B) The purpose for subpoenas issued pursuant to this subsection.
 - (C) The subpoena process.
 - (D) The criteria for the critical infrastructure security risk assessment conducted prior to issuing a subpoena.
 - (E) Policies and procedures on retention and sharing of data obtained by subpoenas.
 - (F) Guidelines on how entities contacted by the Director may respond to notice of a subpoena.
- (11) **ANNUAL REPORTS.**— The Director shall annually submit to the Committee on Homeland Security and Governmental Affairs of the

Senate and the Committee on Homeland Security of the House of Representatives a report (which may include a classified annex but with the presumption of declassification) on the use of subpoenas issued pursuant to this subsection, which shall include the following:

(A) A discussion of the following:

(i) The effectiveness of the use of such subpoenas to mitigate critical infrastructure security vulnerabilities.

(ii) The critical infrastructure security risk assessment process conducted for subpoenas issued under this subsection.

(iii) The number of subpoenas so issued during the preceding year.

(iv) To the extent practicable, the number of vulnerable covered devices or systems mitigated under this subsection by the Agency during the preceding year.

(v) The number of entities notified by the Director under this subsection, and their responses, during the preceding year.

(B) For each subpoena issued pursuant to this subsection, the following:

(i) Information relating to the source of the security vulnerability detected, identified, or received by the Director.

(ii) Information relating to the steps taken to identify the entity at risk prior to issuing the subpoena.

(iii) A description of the outcome of the subpoena, including discussion on the resolution or mitigation of the critical infrastructure security vulnerability.

(12) PUBLICATION OF THE ANNUAL REPORTS.— The Director shall publish a version of the annual report required under paragraph (11) on the website of the Agency, which shall, at a minimum, include the findings described in clauses (iii), (iv), and (v) of subparagraph (A) of such paragraph.

(13) PROHIBITION ON USE OF INFORMATION FOR UNAUTHORIZED PURPOSES.—Any information obtained pursuant to a subpoena issued under this subsection may not be provided to any other Federal department or agency for any purpose other than a cybersecurity purpose or for the purpose of enforcing a subpoena issued pursuant to this subsection.

(q) INDUSTRIAL CONTROL SYSTEMS.—The Director shall maintain capabilities to identify and address threats and vulnerabilities to products and technologies intended for use in the automated control of critical infrastructure processes. In carrying out this subsection, the Director shall—

(1) lead Federal Government efforts, in consultation with Sector Risk Management Agencies, as appropriate, to identify and mitigate

- cybersecurity threats to industrial control systems, including supervisory control and data acquisition systems;
- (2) maintain threat hunting and incident response capabilities to respond to industrial control system cybersecurity risks and incidents;
- (3) provide cybersecurity technical assistance to industry end-users, product manufacturers, Sector Risk Management Agencies, other Federal agencies, and other industrial control system stakeholders to identify, evaluate, assess, and mitigate vulnerabilities;
- (4) collect, coordinate, and provide vulnerability information to the industrial control systems community by, as appropriate, working closely with security researchers, industry endusers, product manufacturers, Sector Risk Management Agencies, other Federal agencies, and other industrial control systems stakeholders; and
- (5) conduct such other efforts and assistance as the Secretary determines appropriate.

(r) COORDINATION ON CYBERSECURITY FOR SLTT ENTITIES.—

(1) COORDINATION.—The Center shall, upon request and to the extent practicable, and in coordination as appropriate with Federal and non-Federal entities, such as the Multi-State Information Sharing and Analysis Center—

- (A) conduct exercises with SLTT entities;
- (B) provide operational and technical cybersecurity training to SLTT entities to address cybersecurity risks or incidents, with or without reimbursement, related to—
 - (i) cyber threat indicators;
 - (ii) defensive measures;
 - (iii) cybersecurity risks;
 - (iv) vulnerabilities; and
 - (v) incident response and management;
- (C) in order to increase situational awareness and help prevent incidents, assist SLTT entities in sharing, in real time, with the Federal Government as well as among SLTT entities, actionable
 - (i) cyber threat indicators;
 - (ii) defensive measures;
 - (iii) information about cybersecurity risks; and (iv) information about incidents;
- (D) provide SLTT entities notifications containing specific incident and malware information that may affect them or their residents;
- (E) provide to, and periodically update, SLTT entities via an easily accessible platform and other means—
 - (i) information about tools;

- (ii) information about products;
 - (iii) resources;
 - (iv) policies;
 - (v) guidelines;
 - (vi) controls; and
 - (vii) other cybersecurity standards and best practices and procedures related to information security, including, as appropriate, information produced by other Federal agencies;
- (F) work with senior SLTT entity officials, including chief information officers and senior election officials and through national associations, to coordinate the effective implementation by SLTT entities of tools, products, resources, policies, guidelines, controls, and procedures related to information security to secure the information systems, including election systems, of SLTT entities;
- (G) provide operational and technical assistance to SLTT entities to implement tools, products, resources, policies, guidelines, controls, and procedures on information security;
- (H) assist SLTT entities in developing policies and procedures for coordinating vulnerability disclosures consistent with international and national standards in the information technology industry; and
- (I) promote cybersecurity education and awareness through engagements with Federal agencies and non-Federal entities.

(s) **REPORT.**—Not later than 1 year after the date of enactment of this subsection, and every 2 years thereafter, the Secretary shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives a report on the services and capabilities that the Agency directly and indirectly provides to SLTT entities.

CYBERSECURITY PLANS

SEC. 2210. [6 U.S.C. § 660]

(a) **DEFINITIONS.**—In this section—

- (1) the term “agency information system” means an information system used or operated by an agency or by another entity on behalf of an agency;
- (2) the terms “cybersecurity risk” and “information system” have the meanings given those terms in section 2209;

(3) the term “intelligence community” has the meaning given the term in section 3(4) of the National Security Act of 1947 (50 U.S.C. 3003(4)); and

(4) the term “national security system” has the meaning given the term in section 11103 of title 40, United States Code.

(b) INTRUSION ASSESSMENT PLAN.—

(1) REQUIREMENT.—The Secretary, in coordination with the Director of the Office of Management and Budget, shall—

(A) develop and implement an intrusion assessment plan to proactively detect, identify, and remove intruders in agency information systems on a routine basis; and

(B) update such plan as necessary.

(2) EXCEPTION.—The intrusion assessment plan required under paragraph (1) shall not apply to the Department of Defense, a national security system, or an element of the intelligence community.

(c) CYBER INCIDENT RESPONSE PLAN.—The Under Secretary appointed under section 103(a)(1)(H) shall, in coordination with appropriate Federal departments and agencies, State and local governments, sector coordinating councils, information sharing and analysis organizations (as defined in section 2222(5)), owners and operators of critical infrastructure, and other appropriate entities and individuals, develop, update not less often than biennially, maintain, and exercise adaptable cyber incident response plans to address cybersecurity risks (as defined in section 2209) to critical infrastructure. The Director, in consultation with relevant Sector Risk Management Agencies and the National Cyber Director, shall develop mechanisms to engage with stakeholders to educate such stakeholders regarding Federal Government cybersecurity roles and responsibilities for cyber incident response.

(d) NATIONAL RESPONSE FRAMEWORK.—The Secretary, in coordination with the heads of other appropriate Federal departments and agencies, and in accordance with the National Cybersecurity Incident Response Plan required under subsection (c), shall regularly update, maintain, and exercise the Cyber Incident Annex to the National Response Framework of the Department.

(e) HOMELAND SECURITY STRATEGY TO IMPROVE THE CYBERSECURITY OF STATE, LOCAL, TRIBAL, AND TERRITORIAL GOVERNMENTS.—

(1) IN GENERAL.—

(A) REQUIREMENT.—Not later than one year after the date of the enactment of this subsection, the Secretary, acting through the Director, shall, in coordination with the heads of appropriate Federal agencies, State, local, Tribal, and territorial governments, and other stakeholders, as appropriate, develop and make publicly available a Homeland Security Strategy to

Improve the Cybersecurity of State, Local, Tribal, and Territorial Governments.

(B) RECOMMENDATIONS AND REQUIREMENTS.—The strategy required under subparagraph (A) shall provide recommendations relating to the ways in which the Federal Government should support and promote the ability of State, local, Tribal, and territorial governments to identify, mitigate against, protect against, detect, respond to, and recover from cybersecurity risks, cybersecurity threats, and incidents (as such term is defined in section 2209).

- (2) CONTENTS.—The strategy required under paragraph (1) shall—
- (A) identify capability gaps in the ability of State, local, Tribal, and territorial governments to identify, protect against, detect, respond to, and recover from cybersecurity risks, cybersecurity threats, incidents, and ransomware incidents;
 - (B) identify Federal resources and capabilities that are available or could be made available to State, local, Tribal, and territorial governments to help those governments identify, protect against, detect, respond to, and recover from cybersecurity risks, cybersecurity threats, incidents, and ransomware incidents;
 - (C) identify and assess the limitations of Federal resources and capabilities available to State, local, Tribal, and territorial governments to help those governments identify, protect against, detect, respond to, and recover from cybersecurity risks, cybersecurity threats, incidents, and ransomware incidents and make recommendations to address such limitations;
 - (D) identify opportunities to improve the coordination of the Agency with Federal and non-Federal entities, such as the Multi-State Information Sharing and Analysis Center, to improve—
 - (i) incident exercises, information sharing and incident notification procedures;
 - (ii) the ability for State, local, Tribal, and territorial governments to voluntarily adapt and implement guidance in Federal binding operational directives; and
 - (iii) opportunities to leverage Federal schedules for cybersecurity investments under section 502 of title 40, United States Code;
 - (E) recommend new initiatives the Federal Government should undertake to improve the ability of State, local, Tribal, and territorial governments to identify, protect against, detect,

respond to, and recover from cybersecurity risks, cybersecurity threats, incidents, and ransomware incidents;

(F) set short-term and long-term goals that will improve the ability of State, local, Tribal, and territorial governments to identify, protect against, detect, respond to, and recover from cybersecurity risks, cybersecurity threats, incidents, and ransomware incidents; and

(G) set dates, including interim benchmarks, as appropriate for State, local, Tribal, and territorial governments to establish baseline capabilities to identify, protect against, detect, respond to, and recover from cybersecurity risks, cybersecurity threats, incidents, and ransomware incidents.

(3) CONSIDERATIONS.—In developing the strategy required under paragraph (1), the Director, in coordination with the heads of appropriate Federal agencies, State, local, Tribal, and territorial governments, and other stakeholders, as appropriate, shall consider—

(A) lessons learned from incidents that have affected State, local, Tribal, and territorial governments, and exercises with Federal and non-Federal entities;

(B) the impact of incidents that have affected State, local, Tribal, and territorial governments, including the resulting costs to such governments;

(C) the information related to the interest and ability of state and non-state threat actors to compromise information systems owned or operated by State, local, Tribal, and territorial governments; and

(D) emerging cybersecurity risks and cybersecurity threats to State, local, Tribal, and territorial governments resulting from the deployment of new technologies.

(4) EXEMPTION.—Chapter 35 of title 44, United States Code (commonly known as the “Paperwork Reduction Act”), shall not apply to any action to implement this subsection.

CLEARANCES

SEC. 2212. [6 U.S.C. § 662]

The Secretary shall make available the process of application for security clearances under Executive Order 13549 (75 Fed. Reg. 162; relating to a classified national security information program) or any successor Executive Order to appropriate representatives of sector coordinating councils, sector information sharing and analysis organizations (as defined in section 2222(5)),

owners and operators of critical infrastructure, and any other person that the Secretary determines appropriate.

NATIONAL ASSET DATABASE

SEC. 2214. [6 U.S.C. § 664]

(a) ESTABLISHMENT.—

(1) NATIONAL ASSET DATABASE.—The Secretary shall establish and maintain a national database of each system or asset that—

(A) the Secretary, in consultation with appropriate homeland security officials of the States, determines to be vital and the loss, interruption, incapacity, or destruction of which would have a negative or debilitating effect on the economic security, public health, or safety of the United States, any State, or any local government; or

(B) the Secretary determines is appropriate for inclusion in the database.

(2) PRIORITIZED CRITICAL INFRASTRUCTURE LIST.—In accordance with Homeland Security Presidential Directive-7, as in effect on January 1, 2007, the Secretary shall establish and maintain a single classified prioritized list of systems and assets included in the database under paragraph (1) that the Secretary determines would, if destroyed or disrupted, cause national or regional catastrophic effects.

(b) USE OF DATABASE.—The Secretary shall use the database established under subsection (a)(1) in the development and implementation of Department plans and programs as appropriate.

(c) MAINTENANCE OF DATABASE.—

(1) IN GENERAL.—The Secretary shall maintain and annually update the database established under subsection (a)(1) and the list established under subsection (a)(2), including—

(A) establishing data collection guidelines and providing such guidelines to the appropriate homeland security official of each State;

(B) regularly reviewing the guidelines established under subparagraph (A), including by consulting with the appropriate homeland security officials of States, to solicit feedback about the guidelines, as appropriate;

(C) after providing the homeland security official of a State with the guidelines under subparagraph (A), allowing the official a reasonable amount of time to submit to the Secretary any data

submissions recommended by the official for inclusion in the database established under subsection (a)(1); (D) examining the contents and identifying any submissions made by such an official that are described incorrectly or that do not meet the guidelines established under subparagraph (A); and (E) providing to the appropriate homeland security official of each relevant State a list of submissions identified under subparagraph (D) for review and possible correction before the Secretary finalizes the decision of which submissions will be included in the database established under subsection (a)(1).

(2) ORGANIZATION OF INFORMATION IN DATABASE.—The Secretary shall organize the contents of the database established under subsection (a)(1) and the list established under subsection (a)(2) as the Secretary determines is appropriate. Any organizational structure of such contents shall include the categorization of the contents—

(A) according to the sectors listed in National Infrastructure Protection Plan developed pursuant to Homeland Security Presidential Directive-7; and

(B) by the State and county of their location.

(3) PRIVATE SECTOR INTEGRATION.—The Secretary shall identify and evaluate methods, including the Department’s Protected Critical Infrastructure Information Program, to acquire relevant private sector information for the purpose of using that information to generate any database or list, including the database established under subsection (a)(1) and the list established under subsection (a)(2).

(4) RETENTION OF CLASSIFICATION.—The classification of information required to be provided to Congress, the Department, or any other department or agency under this section by a sector-specific agency, including the assignment of a level of classification of such information, shall be binding on Congress, the Department, and that other Federal agency.

(d) REPORTS.—

(1) REPORT REQUIRED.—Not later than 180 days after the date of the enactment of the Implementing Recommendations of the 9/11 Commission Act of 2007, and annually thereafter, the Secretary shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives a report on the database established under subsection (a)(1) and the list established under subsection (a)(2).

(2) CONTENTS OF REPORT.—Each such report shall include the following:

(A) The name, location, and sector classification of each of the systems and assets on the list established under subsection (a)(2).

(B) The name, location, and sector classification of each of the systems and assets on such list that are determined by the Secretary to be most at risk to terrorism.

(C) Any significant challenges in compiling the list of the systems and assets included on such list or in the database established under subsection (a)(1).

(D) Any significant changes from the preceding report in the systems and assets included on such list or in such database.

(E) If appropriate, the extent to which such database and such list have been used, individually or jointly, for allocating funds by the Federal Government to prevent, reduce, mitigate, or respond to acts of terrorism.

(F) The amount of coordination between the Department and the private sector, through any entity of the Department that meets with representatives of private sector industries for purposes of such coordination, for the purpose of ensuring the accuracy of such database and such list.

(G) Any other information the Secretary deems relevant.

(3) CLASSIFIED INFORMATION.—The report shall be submitted in unclassified form but may contain a classified annex.

(e) INSPECTOR GENERAL STUDY.—By not later than two years after the date of enactment of the Implementing Recommendations of the 9/11 Commission Act of 2007, the Inspector General of the Department shall conduct a study of the implementation of this section.

(f) NATIONAL INFRASTRUCTURE PROTECTION CONSORTIUM.—The Secretary may establish a consortium to be known as the “National Infrastructure Protection Consortium”. The Consortium may advise the Secretary on the best way to identify, generate, organize, and maintain any database or list of systems and assets established by the Secretary, including the database established under subsection (a)(1) and the list established under subsection (a)(2). If the Secretary establishes the National Infrastructure Protection Consortium, the Consortium may—

(1) be composed of national laboratories, Federal agencies, State and local homeland security organizations, academic institutions, or national Centers of Excellence that have demonstrated experience working with and identifying critical infrastructure and key resources; and

(2) provide input to the Secretary on any request pertaining to the contents of such database or such list.

JOINT CYBER PLANNING OFFICE.

SEC. 2215.

(a) **ESTABLISHMENT OF OFFICE.**—There is established in the Agency an office for joint cyber planning (in this section referred to as the ‘Office’) to develop, for public and private sector entities, plans for cyber defense operations, including the development of a set of coordinated actions to protect, detect, respond to, and recover from cybersecurity risks or incidents or limit, mitigate, or defend against coordinated, malicious cyber operations that pose a potential risk to critical infrastructure or national interests. The Office shall be headed by a senior official of the Agency selected by the Director.

(b) **Planning And Execution.**—In leading the development of plans for cyber defense operations pursuant to subsection (a), the head of the Office shall—

- (1) coordinate with relevant Federal departments and agencies to establish processes and procedures necessary to develop and maintain ongoing coordinated plans for cyber defense operations;
- (2) leverage cyber capabilities and authorities of participating Federal departments and agencies, as appropriate, in furtherance of plans for cyber defense operations;
- (3) ensure that plans for cyber defense operations are, to the greatest extent practicable, developed in collaboration with relevant private sector entities, particularly in areas in which such entities have comparative advantages in limiting, mitigating, or defending against a cybersecurity risk or incident or coordinated, malicious cyber operation;
- (4) ensure that plans for cyber defense operations, as appropriate, are responsive to potential adversary activity conducted in response to United States offensive cyber operations;
- (5) facilitate the exercise of plans for cyber defense operations, including by developing and modeling scenarios based on an understanding of adversary threats to, vulnerability of, and potential consequences of disruption or compromise of critical infrastructure;
- (6) coordinate with and, as necessary, support relevant Federal departments and agencies in the establishment of procedures, development of additional plans, including for offensive and intelligence activities in support of cyber defense operations, and creation of agreements necessary for the rapid execution of plans for cyber defense operations when a cybersecurity risk or incident or malicious cyber operation has been identified; and
- (7) support public and private sector entities, as appropriate, in the execution of plans developed pursuant to this section.

(c) COMPOSITION.—The Office shall be composed of—

- (1) a central planning staff; and
- (2) appropriate representatives of Federal departments and agencies, including—
 - (A) the Department;
 - (B) United States Cyber Command;
 - (C) the National Security Agency;
 - (D) the Federal Bureau of Investigation;
 - (E) the Department of Justice; and
 - (F) the Office of the Director of National Intelligence

(d) CONSULTATION.—In carrying out its responsibilities described in subsection (b), the Office shall regularly consult with appropriate representatives of non-Federal entities, such as—

- (1) State, local, federally-recognized Tribal, and territorial governments;
- (2) information sharing and analysis organizations, including information sharing and analysis centers;
- (3) owners and operators of critical information systems;
- (4) private entities; and
- (5) other appropriate representatives or entities, as determined by the Secretary.

(e) INTERAGENCY AGREEMENTS.—The Secretary and the head of a Federal department or agency referred to in subsection (c) may enter into agreements for the purpose of detailing personnel on a reimbursable or non-reimbursable basis.

(f) DEFINITIONS.—In this section:

- (1) CYBER DEFENSE OPERATIONS.—The term "cyber defense operation" means defensive activities performed for a cybersecurity purpose.
- (2) CYBERSECURITY PURPOSE.—The term "cybersecurity purpose" has the meaning given such term in section 102 of the Cybersecurity Act of 2015 (contained in division N of the Consolidated Appropriations Act, 2016 (Public Law 114–113; 6 U.S.C. 1501)).
- (3) CYBERSECURITY RISK; INCIDENT.—The terms "cybersecurity risk" and "incident" have the meanings given such terms in section 2209.
- (4) INFORMATION SHARING AND ANALYSIS ORGANIZATION.—The term "information sharing and analysis organization" has the meaning given such term in section 2222(5).

**COUNTERINTELLIGENCE AND
SECURITY ENHANCEMENTS ACT OF 1994^[1]**

[Title VIII of the Intelligence Authorization Act for Fiscal Year 1995]
[Public Law 103-359; 108 STAT. 3434; October 14, 1994]

COORDINATION OF COUNTERINTELLIGENCE ACTIVITIES

SEC. 811. [50 U.S.C. § 3381]

(a) **ESTABLISHMENT OF COUNTERINTELLIGENCE POLICY BOARD.**—There is established within the executive branch of Government a National Counterintelligence Policy Board (in this section referred to as the “Board”). The Board shall report to the President through the National Security Council.

(b) **CHAIRPERSON.**—The Director of the National Counterintelligence and Security Center appointed under section 902 of the Counterintelligence Enhancement Act of 2002 (50 U.S.C. 3382) shall serve as the chairperson of the Board.

(c) **MEMBERSHIP.**—The membership of the National Counterintelligence Policy Board shall consist of the following:

- (1) The Director of the National Counterintelligence and Security Center.
- (2) Senior personnel of departments and elements of the United States Government, appointed by the head of the department or element concerned, as follows:

(A) The Department of Justice, including the Federal Bureau of Investigation.

(B) The Department of Defense, including the Joint Chiefs of Staff.

(C) The Department of State.

(D) The Department of Energy.

(E) The Central Intelligence Agency.

(F) Any other department, agency, or element of the United States Government specified by the President.

(d) **FUNCTIONS AND DISCHARGE OF FUNCTIONS.**—

- (1) The Board shall—

(A) serve as the principal mechanism for—

- (i) developing policies and procedures for the approval of the President to govern the conduct of counterintelligence activities; and

¹ Only the select section is included.

(ii) upon the direction of the President, resolving conflicts that arise between elements of the Government conducting such activities; and

(B) act as an interagency working group to—

(i) ensure the discussion and review of matters relating to the implementation of the Counterintelligence Enhancement Act of 2002; and

(ii) provide advice to the Director of the National Counterintelligence and Security Center on priorities in the implementation of the National Counterintelligence Strategy produced pursuant to section 904(e)(2) of that Act (50 U.S.C. 3383(d)(2)).

(2) The Board may, for purposes of carrying out its functions under this section, establish such interagency boards and working groups as the Board considers appropriate.

(e) COORDINATION OF COUNTERINTELLIGENCE MATTERS WITH FEDERAL BUREAU OF INVESTIGATION.—

(1) Except as provided in paragraph (5), the head of each department or agency within the executive branch shall ensure that—

(A) the Federal Bureau of Investigation is advised immediately of any information, regardless of its origin, which indicates that classified information is being, or may have been, disclosed in an unauthorized manner to a foreign power or an agent of a foreign power;

(B) following a report made pursuant to subparagraph (A), the Federal Bureau of Investigation is consulted with respect to all subsequent actions which may be undertaken by the department or agency concerned to determine the source of such loss or compromise; and

(C) where, after appropriate consultation with the department or agency concerned, the Federal Bureau of Investigation undertakes investigative activities to determine the source of the loss or compromise, the Federal Bureau of Investigation is given complete and timely access to the employees and records of the department or agency concerned for purposes of such investigative activities.

(2) Except as provided in paragraph (5), the Director of the Federal Bureau of Investigation shall ensure that espionage information obtained by the Federal Bureau of Investigation pertaining to the personnel, operations, or information of departments or agencies of the executive branch, is provided through appropriate channels in a timely manner to

the department or agency concerned, and that such departments or agencies are consulted in a timely manner with respect to espionage investigations undertaken by the Federal Bureau of Investigation which involve the personnel, operations, or information of such department or agency.

(3)(A) The Director of the Federal Bureau of Investigation shall submit to the head of the department or agency concerned a written assessment of the potential impact of the actions of the department or agency on a counterintelligence investigation.

(B) The head of the department or agency concerned shall—

- (i) use an assessment under subparagraph (A) as an aid in determining whether, and under what circumstances, the subject of an investigation under paragraph (1) should be left in place for investigative purposes; and
- (ii) notify in writing the Director of the Federal Bureau of Investigation of such determination.

(C) The Director of the Federal Bureau of Investigation and the head of the department or agency concerned shall continue to consult, as appropriate, to review the status of an investigation covered by this paragraph, and to reassess, as appropriate, a determination of the head of the department or agency concerned to leave a subject in place for investigative purposes.

(4)(A) The Federal Bureau of Investigation shall notify appropriate officials within the executive branch, including the head of the department or agency concerned, of the commencement of a full field espionage investigation with respect to an employee within the executive branch.

(B) A department or agency may not conduct a polygraph examination, interrogate, or otherwise take any action that is likely to alert an employee covered by a notice under subparagraph (A) of an investigation described in that subparagraph without prior coordination and consultation with the Federal Bureau of Investigation.

(5) Where essential to meet extraordinary circumstances affecting vital national security interests of the United States, the President may on a case-by-case basis waive the requirements of paragraph (1), (2), or (3), as they apply to the head of a particular department or agency, or the Director of the Federal Bureau of Investigation. Such waiver shall be in writing and shall fully state the justification for such waiver. Within thirty days, the President shall notify the Select Committee on Intelligence of the Senate and the Permanent Select Committee on

Intelligence of the House of Representatives that such waiver has been issued, and at that time or as soon as national security considerations permit, provide these committees with a complete explanation of the circumstances which necessitated such waiver.

(6) Nothing in this section may be construed to alter the existing jurisdictional arrangements between the Federal Bureau of Investigation and the Department of Defense with respect to investigations of persons subject to the Uniform Code of Military Justice, nor to impose additional reporting requirements upon the Department of Defense with respect to such investigations beyond those required by existing law and executive branch policy.

(7) As used in this section, the terms “foreign power” and “agent of a foreign power” have the same meanings as set forth in sections 1801(a) and (b), respectively, of this title.

COUNTERINTELLIGENCE ENHANCEMENT ACT OF 2002

[Title IX of the Intelligence Authorization Act for Fiscal Year 2003]
[Public Law 107-306; 116 STAT. 2432; November 27, 2002]

TABLE OF CONTENTS¹

- SEC. 901. Short title; purpose.
- SEC. 902. Director of the National Counterintelligence and Security Center.
- SEC. 903. [Amended Section 811 of the Counterintelligence and Security Enhancements Act of 1994.]
- SEC. 904. National Counterintelligence and Security Center.

SHORT TITLE; PURPOSE

SEC. 901.

(a) **SHORT TITLE.**—This title may be cited as the “Counterintelligence Enhancement Act of 2002”.

(b) **PURPOSE.**—[50 U.S.C. § 3382 note] The purpose of this title is to facilitate the enhancement of the counterintelligence activities of the United States Government by—

- (1) enabling the counterintelligence community of the United States Government to fulfill better its mission of identifying, assessing, prioritizing, and countering the intelligence threats to the United States;
- (2) ensuring that the counterintelligence community of the United States Government acts in an efficient and effective manner; and
- (3) providing for the integration of all the counterintelligence activities of the United States Government.

**DIRECTOR OF THE NATIONAL COUNTERINTELLIGENCE
AND SECURITY CENTER**

SEC. 902. [50 U.S.C. § 3382]

(a) **ESTABLISHMENT.**—There shall be a Director of the National Counterintelligence and Security Center (referred to in this section as the “Director”), who shall be appointed by the President, by and with the advice and consent of the Senate.

(b) **MISSION.**—The mission of the Director shall be to serve as the head of national counterintelligence for the United States Government.

¹ Table of Contents does not appear in the Act itself.

(c) DUTIES.—Subject to the direction and control of the Director of National Intelligence, the duties of the Director are as follows:

- (1) To carry out the mission referred to in subsection (b).
- (2) To act as chairperson of the National Counterintelligence Policy Board established under section 3381 of this title.
- (3) To act as head of the National Counterintelligence and Security Center established under section 3383 of this title.
- (4) To participate as an observer on such boards, committees, and entities of the executive branch as the Director of National Intelligence considers appropriate for the discharge of the mission and functions of the Director and the National Counterintelligence and Security Center under section 3383 of this title.

[SEC. 903. Amended Section 811 of the Counterintelligence and Security Enhancements Act of 1994.]

NATIONAL COUNTERINTELLIGENCE AND SECURITY CENTER

SEC. 904. [50 U.S.C. § 3383]

(a) ESTABLISHMENT.—There shall be a National Counterintelligence and Security Center.

(b) HEAD OF CENTER.—The Director of the National Counterintelligence and Security Center shall be the head of the National Counterintelligence and Security Center.

(c) LOCATION OF CENTER.—The National Counterintelligence and Security Center shall be located in the Office of the Director of National Intelligence.

(d) MISSION.—The mission of the National Counterintelligence and Security Center shall include organizing and leading strategic planning for counterintelligence activities of the United States Government by integrating instruments of national power as needed to counter foreign intelligence activities.

(e) FUNCTIONS.—Subject to the direction and control of the Director of the National Counterintelligence and Security Center, the functions of the National Counterintelligence and Security Center shall be as follows:

(1) NATIONAL THREAT IDENTIFICATION AND PRIORITIZATION ASSESSMENT.—Subject to subsection (f), in consultation with appropriate department and agencies of the United States Government, and private sector entities, to produce a strategic planning assessment of the counterintelligence requirements of the United States to be known as the National Threat Identification and Prioritization Assessment.

(2) NATIONAL COUNTERINTELLIGENCE STRATEGY.—

(A) REQUIREMENT TO PRODUCE.—Subject to subsection (f), in consultation with appropriate department and agencies of the United States Government, and private sector entities, and based on the most current National Threat Identification and Prioritization Assessment under paragraph (1), to produce a strategy for the counterintelligence programs and activities of the United States Government to be known as the National Counterintelligence Strategy.

(B) REVISION AND REQUIREMENT.—The National Counterintelligence Strategy shall be revised or updated at least once every three years and shall be aligned with the strategy and policies of the Director of National Intelligence.

(3) IMPLEMENTATION OF NATIONAL COUNTERINTELLIGENCE STRATEGY.—To evaluate on an ongoing basis the implementation of the National Counterintelligence Strategy and to submit to the President periodic reports on such evaluation, including a discussion of any shortfalls in the implementation of the Strategy and recommendations for remedies for such shortfalls.

(4) NATIONAL COUNTERINTELLIGENCE STRATEGIC ANALYSES.—As directed by the Director of National Intelligence and in consultation with appropriate elements of the departments and agencies of the United States Government, to oversee and coordinate the production of strategic analyses of counterintelligence matters, including the production of counterintelligence damage assessments and assessments of lessons learned from counterintelligence activities.

(5) NATIONAL COUNTERINTELLIGENCE PROGRAM BUDGET.—At the direction of the Director of National Intelligence—

(A) to coordinate the development of budgets and resource allocation plans for the counterintelligence programs and activities of the Department of Defense, the Federal Bureau of Investigation, the Central Intelligence Agency, and other appropriate elements of the United States Government;

(B) to ensure that the budgets and resource allocation plans developed under subparagraph (A) address the objectives and priorities for counterintelligence under the National Counterintelligence Strategy; and

(C) to submit to the National Security Council periodic reports on the activities undertaken by the Office under subparagraphs (A) and (B).

(6) NATIONAL COUNTERINTELLIGENCE COLLECTION AND TARGETING COORDINATION.—To develop priorities for counterintelligence

investigations and operations, and for collection of counterintelligence, for purposes of the National Counterintelligence Strategy, except that the National Counterintelligence and Security Center may not—

(A) carry out any counterintelligence investigations or operations; or

(B) establish its own contacts, or carry out its own activities, with foreign intelligence services.

(7) NATIONAL COUNTERINTELLIGENCE OUTREACH, WATCH, AND WARNING.—

(A) COUNTERINTELLIGENCE VULNERABILITY ASSESSMENTS AND SURVEYS.—To develop standards and criteria for counterintelligence risk assessments and surveys of the vulnerability of the United States to intelligence threats, including with respect to critical infrastructure and critical technologies, in order to identify the areas, programs, and activities that require protection from such threats.

(B) OUTREACH.—To carry out and coordinate outreach programs and activities on counterintelligence to other elements of the United States Government, and the private sector, and to coordinate the dissemination to the public of warnings on intelligence threats to the United States.

(C) RESEARCH AND DEVELOPMENT.—To ensure that research and development programs and activities of the United States Government, and the private sector, direct attention to the needs of the counterintelligence community for technologies, products, and services.

(D) TRAINING AND PROFESSIONAL DEVELOPMENT.—To develop policies and standards for training and professional development of individuals engaged in counterintelligence activities and to manage the conduct of joint training exercises for such personnel.

(E) VULNERABILITIES FROM FOREIGN COMMERCIAL SPYWARE.—

(i) Consultation.—In carrying out efforts to secure covered devices, to consult with the private sector of the United States and reputable third-party researchers to identify vulnerabilities from foreign commercial spyware (as defined in section 1102A(a) of the National Security Act of 1947) and maintain effective security measures for such devices.

(ii) Covered device defined.—In this subparagraph, the term 'covered device' means any electronic mobile device

including smartphones, tablet computing devices, or laptop computing devices, that is issued by an element of the intelligence community for official use.

(f) **ADDITIONAL REQUIREMENTS REGARDING NATIONAL THREAT IDENTIFICATION AND PRIORITIZATION ASSESSMENT AND NATIONAL COUNTERINTELLIGENCE STRATEGY.**—

(1) A National Threat Identification and Prioritization Assessment under subsection (e)(1), and any modification of such assessment, shall not go into effect until approved by the President.

(2) A National Counterintelligence Strategy under subsection (e)(2), and any modification of such strategy, shall not go into effect until approved by the President.

(3) The National Counterintelligence Executive shall submit to the congressional intelligence committees each National Threat Identification and Prioritization Assessment, or modification thereof, and each National Counterintelligence Strategy, or modification thereof, approved under this section.

(4) In this subsection, the term “congressional intelligence committees” means—

- (A) the Select Committee on Intelligence of the Senate; and
- (B) the Permanent Select Committee on Intelligence of the House of Representatives.

(g) **PERSONNEL.**—

(1) Personnel of the National Counterintelligence and Security Center may consist of personnel employed by the Center or personnel on detail from any other department, agency, or element of the Federal Government. Any such detail may be on a reimbursable or nonreimbursable basis, at the election of the head of the agency detailing such personnel.

(2) Notwithstanding section 104(d)1 or any other provision of law limiting the period of the detail of personnel on a nonreimbursable basis, the detail of an officer or employee of United States or a member of the Armed Forces under paragraph (1) on a nonreimbursable basis may be for any period in excess of one year that the Director of the National Counterintelligence and Security Center and the head of the department, agency, or element concerned consider appropriate.

(h) **TREATMENT OF ACTIVITIES UNDER CERTAIN ADMINISTRATIVE LAWS.**—The files of the National Counterintelligence and Security Center shall be treated as operational files of the Central Intelligence Agency for purposes of section 701 of the National Security Act of 1947 (50 U.S.C. 3141) to the extent such files

meet criteria under subsection (b) of that section for treatment of files as operational files of an element of the Agency.

(i) OVERSIGHT BY CONGRESS.—The location of the National Counterintelligence and Security Center within the Office of the Director of National Intelligence shall not be construed as affecting access by Congress, or any committee of Congress, to—

(1) any information, document, record, or paper in the possession of the Center; or

(2) any personnel of the Center.

(j) CONSTRUCTION.—Nothing in this section shall be construed as affecting the authority of the Director of National Intelligence, the Secretary of Defense, the Secretary of State, the Attorney General, or the Director of the Federal Bureau of Investigation as provided or specified under the National Security Act of 1947 or under other provisions of law.

CLASSIFIED INFORMATION PROCEDURES ACT

[Public Law 96–456; 94 STAT. 2025; October 15, 1980]

AN ACT To provide certain pretrial, trial, and appellate procedures for criminal cases involving classified information.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

TABLE OF CONTENTS¹

SEC. 1.	Definitions.
SEC. 2.	Pretrial conference.
SEC. 3.	Protective orders.
SEC. 4.	Discovery of classified information by defendants.
SEC. 5.	Notice of defendant’s intention to disclose classified information.
SEC. 6.	Procedures for cases involving classified information.
SEC. 7.	Interlocutory appeal.
SEC. 8.	Introduction of classified information.
SEC. 9.	Security procedures.
SEC. 9A.	Coordination requirements relating to the prosecution of cases involving classified information.
SEC. 10.	Identification of information related to national defense.
SEC. 11.	Amendment to the Act.
SEC. 12.	Attorney General guidelines.
SEC. 13.	Reports to Congress.
SEC. 14.	Functions of Attorney General may be exercised by Deputy Attorney General, the Associate Attorney General, or a designated Assistant Attorney General.
SEC. 15.	Effective date.
SEC. 16.	Short title.

DEFINITIONS

SECTION 1. [18 U.S.C. App. § 1]

(a) “Classified information”, as used in this Act, means any information or material that has been determined by the United States Government pursuant to an Executive order, statute, or regulation, to require protection against

¹ Table of Contents does not appear in the Act itself.

unauthorized disclosure for reasons of national security and any restricted data, as defined in paragraph r. of section 11 of the Atomic Energy Act of 1954 (42 U.S.C. 2014(y)).

(b) “National security”, as used in this Act, means the national defense and foreign relations of the United States.

PRETRIAL CONFERENCE

SEC. 2. [18 U.S.C. App. § 2]

At any time after the filing of the indictment or information, any party may move for a pretrial conference to consider matters relating to classified information that may arise in connection with the prosecution. Following such motion, or on its own motion, the court shall promptly hold a pretrial conference to establish the timing of requests for discovery, the provision of notice required by section 5 of this Act, and the initiation of the procedure established by section 6 of this Act. In addition, at the pretrial conference the court may consider any matters which relate to classified information or which may promote a fair and expeditious trial. No admission made by the defendant or by any attorney for the defendant at such a conference may be used against the defendant unless the admission is in writing and is signed by the defendant and by the attorney for the defendant.

PROTECTIVE ORDERS

SEC. 3. [18 U.S.C. App. § 3]

Upon motion of the United States, the court shall issue an order to protect against the disclosure of any classified information disclosed by the United States to any defendant in any criminal case in a district court of the United States.

DISCOVERY OF CLASSIFIED INFORMATION BY DEFENDANTS

SEC. 4. [18 U.S.C. App. § 4]

The court, upon a sufficient showing, may authorize the United States to delete specified items of classified information from documents to be made available to the defendant through discovery under the Federal Rules of Criminal Procedure, to substitute a summary of the information for such classified documents, or to substitute a statement admitting relevant facts that the classified information would tend to prove. The court may permit the United States to make a request for such authorization in the form of a written statement to be inspected by the court alone. If the court enters an order granting relief following such an ex parte showing, the entire text of the statement of the United States shall be sealed and

preserved in the records of the court to be made available to the appellate court in the event of an appeal.

**NOTICE OF DEFENDANT'S INTENTION TO DISCLOSE
CLASSIFIED INFORMATION**

SEC. 5. [18 U.S.C. App. § 5]

(a) NOTICE BY DEFENDANT.—If a defendant reasonably expects to disclose or to cause the disclosure of classified information in any manner in connection with any trial or pretrial proceeding involving the criminal prosecution of such defendant, the defendant shall, within the time specified by the court or, where no time is specified, within thirty days prior to trial, notify the attorney for the United States and the court in writing. Such notice shall include a brief description of the classified information. Whenever a defendant learns of additional classified information he reasonably expects to disclose at any such proceeding, he shall notify the attorney for the United States and the court in writing as soon as possible thereafter and shall include a brief description of the classified information. No defendant shall disclose any information known or believed to be classified in connection with a trial or pretrial proceeding until notice has been given under this subsection and until the United States has been afforded a reasonable opportunity to seek a determination pursuant to the procedure set forth in section 6 of this Act, and until the time for the United States to appeal such determination under section 7 has expired or any appeal under section 7 by the United States is decided.

(b) FAILURE TO COMPLY.—If the defendant fails to comply with the requirements of subsection (a) the court may preclude disclosure of any classified information not made the subject of notification and may prohibit the examination by the defendant of any witness with respect to any such information.

PROCEDURES FOR CASES INVOLVING CLASSIFIED INFORMATION

SEC. 6. [18 U.S.C. App. § 6]

(a) MOTION FOR HEARING.—Within the time specified by the court for the filing of a motion under this section, the United States may request the court to conduct a hearing to make all determinations concerning the use, relevance, or admissibility of classified information that would otherwise be made during the trial or pretrial proceeding. Upon such a request, the court shall conduct such a hearing. Any hearing held pursuant to this subsection (or any portion of such hearing specified in the request of the Attorney General) shall be held in camera if the Attorney General certifies to the court in such petition that a public

proceeding may result in the disclosure of classified information. As to each item of classified information, the court shall set forth in writing the basis for its determination. Where the United States' motion under this subsection is filed prior to the trial or pretrial proceeding, the court shall rule prior to the commencement of the relevant proceeding.

(b) NOTICE.—

(1) Before any hearing is conducted pursuant to a request by the United States under subsection (a), the United States shall provide the defendant with notice of the classified information that is at issue. Such notice shall identify the specific classified information at issue whenever that information previously has been made available to the defendant by the United States. When, the United States has not previously made the information available to the defendant in connection with the case, the information may be described by generic category, in such form as the court may approve, rather than by identification of the specific information of concern to the United States.

(2) Whenever the United States requests a hearing under subsection (a), the court, upon request of the defendant, may order the United States to provide the defendant, prior to trial, such details as to the portion of the indictment or information at issue in the hearing as are needed to give the defendant fair notice to prepare for the hearing.

(c) ALTERNATIVE PROCEDURE FOR DISCLOSURE OF CLASSIFIED INFORMATION.—

(1) Upon any determination by the court authorizing the disclosure of specific classified information under the procedures established by this section, the United States may move that, in lieu of the disclosure of such specific classified information, the court order—

(A) the substitution for such classified information of a statement admitting relevant facts that the specific classified information would tend to prove; or

(B) the substitution for such classified information of a summary of the specific classified information. The court shall grant such a motion of the United States if it finds that the statement or summary will provide the defendant with substantially the same ability to make his defense as would disclosure of the specific classified information. The court shall hold a hearing on any motion under this section. Any such hearing shall be held in camera at the request of the Attorney General.

(2) The United States may, in connection with a motion under paragraph (1), submit to the court an affidavit of the Attorney General certifying that disclosure of classified information would cause identifiable damage

CLASSIFIED INFORMATION PROCEDURES ACT

to the national security of the United States and explaining the basis for the classification of such information. If so requested by the United States, the court shall examine such affidavit in camera and ex parte.

(d) **SEALING OF RECORDS OF IN CAMERA HEARINGS.**—If at the close of an in camera hearing under this Act (or any portion of a hearing under this Act that is held in camera) the court determines that the classified information at issue may not be disclosed or elicited at the trial or pretrial proceeding, the record of such in camera hearing shall be sealed and preserved by the court for use in the event of an appeal. The defendant may seek reconsideration of the court’s determination prior to or during trial.

(e) **PROHIBITION ON DISCLOSURE OF CLASSIFIED INFORMATION BY DEFENDANT, RELIEF FOR DEFENDANT WHEN UNITED STATES OPPOSES DISCLOSURE.**—

(1) Whenever the court denies a motion by the United States that it issue an order under subsection (c) and the United States files with the court an affidavit of the Attorney General objecting to disclosure of the classified information at issue, the court shall order that the defendant not disclose or cause the disclosure of such information.

(2) Whenever a defendant is prevented by an order under paragraph (1) from disclosing or causing the disclosure of classified information, the court shall dismiss the indictment or information; except that, when the court determines that the interests of justice would not be served by dismissal of the indictment or information, the court shall order such other action, in lieu of dismissing the indictment or information, as the court determines is appropriate. Such action may include, but need not be limited to—

(A) dismissing specified counts of the indictment or information;

(B) finding against the United States on any issue as to which the excluded classified information relates; or

(C) striking or precluding all or part of the testimony of a witness.

An order under this paragraph shall not take effect until the court has afforded the United States an opportunity to appeal such order under section 7, and thereafter to withdraw its objection to the disclosure of the classified information at issue.

(f) **RECIPROCITY.**—Whenever the court determines pursuant to subsection (a) that classified information may be disclosed in connection with a trial or pretrial proceeding, the court shall, unless the interests of fairness do not so require, order the United States to provide the defendant with the information it expects to use to rebut the classified information. The court may place the United States under a continuing duty to disclose such rebuttal information. If the United States fails to comply with its obligation under this subsection, the court may exclude any evidence not made the subject of a required disclosure and may prohibit the

examination by the United States of any witness with respect to such information.

INTERLOCUTORY APPEAL

SEC. 7. [18 U.S.C. App. § 7]

(a) An interlocutory appeal by the United States taken before or after the defendant has been placed in jeopardy shall lie to a court of appeals from a decision or order of a district court in a criminal case authorizing the disclosure of classified information, imposing sanctions for nondisclosure of classified information, or refusing a protective order sought by the United States to prevent the disclosure of classified information.

(b) An appeal taken pursuant to this section either before or during trial shall be expedited by the court of appeals. Prior to trial, an appeal shall be taken within fourteen days after the decision or order appealed from and the trial shall not commence until the appeal is resolved. If an appeal is taken during trial, the trial court shall adjourn the trial until the appeal is resolved and the court of appeals (1) shall hear argument on such appeal within four days of the adjournment of the trial, excluding intermediate weekends and holidays, (2) may dispense with written briefs other than the supporting materials previously submitted to the trial court, (3) shall render its decision within four days of argument on appeal, excluding intermediate weekends and holidays, and (4) may dispense with the issuance of a written opinion in rendering its decision. Such appeal and decision shall not affect the right of the defendant, in a subsequent appeal from a judgment of conviction, to claim as error reversal by the trial court on remand of a ruling appealed from during trial.

INTRODUCTION OF CLASSIFIED INFORMATION

SEC. 8. [18 U.S.C. App. § 8]

(a) **CLASSIFICATION STATUS.**—Writings, recordings, and photographs containing classified information may be admitted into evidence without change in their classification status.

(b) **PRECAUTIONS BY COURT.**—The court, in order to prevent unnecessary disclosure of classified information involved in any criminal proceeding, may order admission into evidence of only part of a writing, recording, or photograph, or may order admission into evidence of the whole writing, recording, or photograph with excision of some or all of the classified information contained therein, unless the whole ought in fairness be considered.

(c) **TAKING OF TESTIMONY.**—During the examination of a witness in any criminal proceeding, the United States may object to any question or line of

inquiry that may require the witness to disclose classified information not previously found to be admissible. Following such an objection, the court shall take such suitable action to determine whether the response is admissible as will safeguard against the compromise of any classified information. Such action may include requiring the United States to provide the court with a proffer of the witness' response to the question or line of inquiry and requiring the defendant to provide the court with a proffer of the nature of the information he seeks to elicit.

SECURITY PROCEDURES

SEC. 9. [18 U.S.C. App. § 9]

(a) Within one hundred and twenty days of the date of the enactment of this Act, the Chief Justice of the United States, in consultation with the Attorney General, the Director of National Intelligence, and the Secretary of Defense, shall prescribe rules establishing procedures for the protection against unauthorized disclosure of any classified information in the custody of the United States district courts, courts of appeal, or Supreme Court. Such rules, and any changes in such rules, shall be submitted to the appropriate committees of Congress and shall become effective forty-five days after such submission.

(b) Until such time as rules under subsection (a) first become effective, the Federal courts shall in each case involving classified information adopt procedures to protect against the unauthorized disclosure of such information.

COORDINATION REQUIREMENTS RELATING TO THE PROSECUTION OF CASES INVOLVING CLASSIFIED INFORMATION

SEC. 9A. [18 U.S.C. App. § 9A]

(a) **BRIEFINGS REQUIRED.**—The Assistant Attorney General for the Criminal Division or the Assistant Attorney General for National Security, as appropriate, and the appropriate United States attorney, or the designees of such officials, shall provide briefings to the senior agency official, or the designee of such official, with respect to any case involving classified information that originated in the agency of such senior agency official.

(b) **TIMING OF BRIEFINGS.**—Briefings under subsection (a) with respect to a case shall occur—

- (1) as soon as practicable after the Department of Justice and the United States attorney concerned determine that a prosecution or potential prosecution could result; and
- (2) at such other times thereafter as are necessary to keep the senior agency official concerned fully and currently informed of the status of the prosecution.

(c) SENIOR AGENCY OFFICIAL DEFINED.—In this section, the term “senior agency official” has the meaning given that term in section 1.1 of Executive Order No. 12958.

IDENTIFICATION OF INFORMATION RELATED TO NATIONAL DEFENSE

SEC. 10. [18 U.S.C. App. § 10]

In any prosecution in which the United States must establish that material relates to the national defense or constitutes classified information, the United States shall notify the defendant, within the time before trial specified by the court, of the portions of the material that it reasonably expects to rely upon to establish the national defense or classified information element of the offense.

AMENDMENT TO THE ACT

SEC. 11. [18 U.S.C. App. § 11]

Sections 1 through 10 of this Act may be amended as provided in section 2076, title 28, United States Code.

ATTORNEY GENERAL GUIDELINES

SEC. 12. [18 U.S.C. App. § 12]

(a) Within one hundred and eighty days of enactment of this Act, the Attorney General shall issue guidelines specifying the factors to be used by the Department of Justice in rendering a decision whether to prosecute a violation of Federal law in which, in the judgment of the Attorney General, there is a possibility that classified information will be revealed. Such guidelines shall be transmitted to the appropriate committees of Congress.

(b) When the Department of Justice decides not to prosecute a violation of Federal law pursuant to subsection (a), an appropriate official of the Department of Justice shall prepare written findings detailing the reasons for the decision not to prosecute. The findings shall include—

- (1) the intelligence information which the Department of Justice officials believe might be disclosed,
- (2) the purpose for which the information might be disclosed,
- (3) the probability that the information would be disclosed, and
- (4) the possible consequences such disclosure would have on the national security.

REPORTS TO CONGRESS

SEC. 13. [18 U.S.C. App. § 13]

(a) Consistent with applicable authorities and duties, including those conferred by the Constitution upon the executive and legislative branches, the Attorney General shall report orally or in writing semiannually to the Permanent Select Committee on Intelligence of the United States House of Representatives, the Select Committee on Intelligence of the United States Senate, and the chairmen and ranking minority members of the Committees on the Judiciary of the Senate and House of Representatives on all cases where a decision not to prosecute a violation of Federal law pursuant to section 12(a) has been made.

(b) In the case of the semiannual reports (whether oral or written) required to be submitted under subsection (a) to the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate, the submittal dates for such reports shall be as provided in section 507 of the National Security Act of 1947.

(c) The Attorney General shall deliver to the appropriate committees of Congress a report concerning the operation and effectiveness of this Act and including suggested amendments to this Act. For the first three years this Act is in effect, there shall be a report each year. After three years, such reports shall be delivered as necessary.

FUNCTIONS OF ATTORNEY GENERAL MAY BE EXERCISED BY DEPUTY ATTORNEY GENERAL, THE ASSOCIATE ATTORNEY GENERAL, OR A DESIGNATED ASSISTANT ATTORNEY GENERAL

SEC. 14. [18 U.S.C. App. § 14]

The functions and duties of the Attorney General under this Act may be exercised by the Deputy Attorney General, the Associate Attorney General, or by an Assistant Attorney General designated by the Attorney General for such purpose and may not be delegated to any other official.

EFFECTIVE DATE

SEC. 15. [18 U.S.C. App. § 15]

The provisions of this Act shall become effective upon the date of the enactment of this Act, but shall not apply to any prosecution in which an indictment or information was filed before such date.

CLASSIFIED INFORMATION PROCEDURES ACT

SHORT TITLE

SEC. 16. [18 U.S.C. App. § 16]

That this Act may be cited as the “Classified Information Procedures Act”.

FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978

[Public Law 95–511; 92 STAT. 1783; October 25, 1978]

AN ACT To authorize electronic surveillance to obtain foreign intelligence information.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SHORT TITLE

That this Act may be cited as the “Foreign Intelligence Surveillance Act of 1978”.

TABLE OF CONTENTS

**TITLE I—ELECTRONIC SURVEILLANCE WITHIN THE UNITED STATES
FOR FOREIGN INTELLIGENCE PURPOSES**

SEC. 101.	Definitions.
SEC. 102.	Authorization for electronic surveillance for foreign intelligence purposes.
SEC. 103.	Designation of judges.
SEC. 104.	Application for an order.
SEC. 105.	Issuance of an order.
SEC. 106.	Use of information.
SEC. 107.	Report of electronic surveillance.
SEC. 108.	Congressional oversight.
SEC. 109.	Penalties.
SEC. 110.	Civil liability.
SEC. 110A.	Reporting requirements for civil actions.
SEC. 111.	Authorization during time of war.
SEC. 112.	Statement of exclusive means by which electronic surveillance and interception of certain communications may be conducted.

TITLE II—CONFORMING AMENDMENTS

SEC. 201.	Amendments to chapter 119 of title 18, United States Code.
-----------	--

TITLE III—PHYSICAL SEARCHES WITHIN THE UNITED STATES
FOR FOREIGN INTELLIGENCE PURPOSES

- SEC. 301. Definitions.
- SEC. 302. Authorization of physical searches for foreign intelligence purposes.
- SEC. 303. Application for an order.
- SEC. 304. Issuance of an order.
- SEC. 305. Use of information.
- SEC. 306. Congressional oversight.
- SEC. 307. Penalties.
- SEC. 308. Civil liability.
- SEC. 309. Authorization during time of war.

TITLE IV—PEN REGISTERS AND TRAP AND TRACE DEVICES
FOR FOREIGN INTELLIGENCE PURPOSES

- SEC. 401. Definitions.
- SEC. 402. Pen registers and trap and trace devices for foreign intelligence and international terrorism investigations.
- SEC. 403. Authorization during emergencies.
- SEC. 404. Authorization during time of war.
- SEC. 405. Use of information.
- SEC. 406. Congressional oversight.

TITLE V—ACCESS TO CERTAIN BUSINESS RECORDS FOR
FOREIGN INTELLIGENCE PURPOSES

- SEC. 501. Definitions.
- SEC. 502. Access to certain business records for foreign intelligence and international terrorism investigations.
- SEC. 503. Congressional oversight.

TITLE VI—OVERSIGHT

- SEC. 601. Semiannual report of the Attorney General.
- SEC. 602. Declassification of significant decisions, orders, and opinions.
- SEC. 603. Annual reports.
- SEC. 604. Public reporting by persons subject to orders.

TITLE VII—ADDITIONAL PROCEDURES REGARDING CERTAIN
PERSONS OUTSIDE THE UNITED STATES

- SEC. 701. Definitions.
- SEC. 702. Procedures for targeting certain persons outside the United States other than United States persons.
- SEC. 703. Certain acquisitions inside the United States targeting United States persons outside the United States.
- SEC. 704. Other acquisitions targeting United States persons outside the United States.
- SEC. 705. Joint applications and concurrent authorizations.
- SEC. 706. Use of information acquired under title VII.
- SEC. 707. Congressional oversight.
- SEC. 708. Savings provision
- SEC. 709. Penalties for unauthorized disclosure.

TITLE VIII – PROTECTION OF PERSONS ASSISTING THE GOVERNMENT

- SEC. 801. Definitions.
- SEC. 802. Procedures for implementing statutory defenses.
- SEC. 803. Preemption.
- SEC. 804. Reporting.

SELECTED ADDITIONAL PROVISIONS OF THE FISA AMENDMENTS
ACT OF 2008¹

- SEC. 301. Review of Previous Actions.
- SEC. 401. Severability.
- SEC. 404. Transition Procedures.

SELECTED ADDITIONAL SAVING PROVISIONS²

- Pub. L. 108-458, 118 STAT. 3638, § 6001(b)
- Pub. L. 107-56, 115 STAT. 227, 295 § 22
- Pub. L. 116-69, 133 STAT. 1134, 1143, § 1703(b)
- Pub. L. 109-177, 120 STAT. 192, 195
- Pub. L. 116-69, 133 STAT. 1134, 1143, § 1703(a)

¹ This section of the Table of Contents does not appear in the Act itself.

² This section of the Table of Contents does not appear in the Act itself.

TITLE I—ELECTRONIC SURVEILLANCE WITHIN THE UNITED STATES FOR FOREIGN INTELLIGENCE PURPOSES

DEFINITIONS

SECTION 101. [50 U.S.C. § 1801]

As used in this title:

(a) “Foreign power” means—

- (1) a foreign government or any component, thereof, whether or not recognized by the United States;
- (2) a faction of a foreign nation or nations, not substantially composed of United States persons;
- (3) an entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments;
- (4) a group engaged in international terrorism or activities in preparation therefor;
- (5) a foreign-based political organization, not substantially composed of United States persons;
- (6) an entity that is directed and controlled by a foreign government or governments; or
- (7) an entity not substantially composed of United States persons that is engaged in the international proliferation of weapons of mass destruction.

(b) “Agent of a foreign power” means—

- (1) any person other than a United States person, who—
 - (A) acts in the United States as an officer or employee of a foreign power, or as a member of a foreign power as defined in subsection (a)(4), irrespective of whether the person is inside the United States;
 - (B) acts for or on behalf of a foreign power which engages in clandestine intelligence activities in the United States contrary to the interests of the United States, when the circumstances indicate that such person may engage in such activities, or when such person knowingly aids or abets any person in the conduct of such activities or knowingly conspires with any person to engage in such activities;
 - (C) [This provision expired on March 15, 2020]
 - (D) engages in the international proliferation of weapons of mass destruction, or activities in preparation therefor; or

(E) engages in the international proliferation of weapons of mass destruction, or activities in preparation therefor, for or on behalf of a foreign power, or knowingly aids or abets any person in the conduct of such proliferation or activities in preparation therefor, or knowingly conspires with any person to engage in such proliferation or activities in preparation therefor; or

(2) any person who—

(A) knowingly engages in clandestine intelligence gathering activities for or on behalf of a foreign power, which activities involve or may involve a violation of the criminal statutes of the United States;

(B) pursuant to the direction of an intelligence service or network of a foreign power, knowingly engages in any other clandestine intelligence activities for or on behalf of such foreign power, which activities involve or are about to involve a violation of the criminal statutes of the United States;

(C) knowingly engages in sabotage or international terrorism, or activities that are in preparation therefor, for or on behalf of a foreign power;

(D) knowingly enters the United States under a false or fraudulent identity for or on behalf of a foreign power or, while in the United States, knowingly assumes a false or fraudulent identity for or on behalf of a foreign power; or

(E) knowingly aids or abets any person in the conduct of activities described in subparagraph (A), (B), or (C) or knowingly conspires with any person to engage in activities described in subparagraph (A), (B), or (C).

(c) “International terrorism” means activities that—

(1) involve violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States or of any State, or that would be a criminal violation if committed within the jurisdiction of the United States or any State;

(2) appear to be intended—

(A) to intimidate or coerce a civilian population;

(B) to influence the policy of a government by intimidation or coercion; or

(C) to affect the conduct of a government by assassination or kidnapping; and

(3) occur totally outside the United States, or transcend national boundaries in terms of the means by which they are accomplished, the

persons they appear intended to coerce or intimidate, or the locale in which their perpetrators operate or seek asylum.

(d) “Sabotage” means activities that involve a violation of chapter 105 of title 18, United States Code, or that would involve such a violation if committed against the United States.

(e) “Foreign intelligence information” means—

(1) information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against—

(A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;

(B) sabotage, international terrorism, or the international proliferation of weapons of mass destruction by a foreign power or an agent of a foreign power;

(C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power;

or

(D) international production, distribution, or financing of illicit synthetic drugs, opioids, cocaine, or other drugs driving overdose deaths, or precursors of any aforementioned; or

(2) information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to—

(A) the national defense or the security of the United States; or

(B) the conduct of the foreign affairs of the United States.

(f) “Electronic surveillance” means—

(1) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire or radio communications sent by or intended to be received by a particular, known United States person who is in the United States, if the contents are acquired by intentionally targeting that United States person, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes;

(2) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire communication to or from a person in the United States, without the consent of any party thereto, if such acquisition occurs in the United States, but does not include the acquisition of those communications of computer trespassers that would be permissible under section 2511(2)(i) of title 18, United States Code;

(3) the intentional acquisition by an electronic, mechanical, or other surveillance device of the contents of any radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if

both the sender and all intended recipients are located within the United States; or

(4) the installation or use of an electronic, mechanical, or other surveillance device in the United States for monitoring to acquire information, other than from a wire or radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes.

(g) “Attorney General” means the Attorney General of the United States (or Acting Attorney General), the Deputy Attorney General, or, upon the designation of the Attorney General, the Assistant Attorney General designated as the Assistant Attorney General for National Security under section 507A of title 28, United States Code.

(h) “Minimization procedures”, with respect to electronic surveillance, means—
(1) specific procedures, which shall be adopted by the Attorney General, that are reasonably designed in light of the purpose and technique of the particular surveillance, to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information;

(2) procedures that require that nonpublicly available information, which is not foreign intelligence information, as defined in subsection (e)(1), shall not be disseminated in a manner that identifies any United States person, without such person’s consent, unless such person’s identity is necessary to understand foreign intelligence information or assess its importance;

(3) notwithstanding paragraphs (1) and (2), procedures that allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes; and

(4) notwithstanding paragraphs (1), (2), and (3), with respect to any electronic surveillance approved pursuant to section 102(a), procedures that require that no contents of any communication to which a United States person is a party shall be disclosed, disseminated, or used for any purpose or retained for longer than 72 hours unless a court order under section 105 is obtained or unless the Attorney General determines that the information indicates a threat of death or serious bodily harm to any person.

(i) “United States person” means a citizen of the United States, an alien lawfully admitted for permanent residence (as defined in section 101(a)(20) of the Immigration and Nationality Act), an unincorporated association a substantial

number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States, but does not include a corporation or an association which is a foreign power, as defined in subsection (a)(1), (2), or (3).

(j) “United States”, when used in a geographic sense, means all areas under the territorial sovereignty of the United States and the Trust Territory of the Pacific Islands.

(k) “Aggrieved person” means a person who is the target of an electronic surveillance or any other person whose communications or activities were subject to electronic surveillance.

(l) “Wire communication” means any communications while it is being carried by a wire, cable, or other like connection furnished or operated by any person engaged as a common carrier in providing or operating such facilities for the transmission of interstate or foreign communications.

(m) “Person” means any individual, including any officer or employee of the Federal Government, or any group, entity, association, corporation, or foreign power.

(n) “Contents”, when used with respect to a communication, includes any information concerning the identity of the parties to such communications or the existence, substance, purport, or meaning of that communication.

(o) “State” means any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, the Trust Territory of the Pacific Islands, and any territory or possession of the United States.

(p) “Weapon of mass destruction” means—

(1) any explosive, incendiary, or poison gas device that is designed, intended, or has the capability to cause a mass casualty incident;

(2) any weapon that is designed, intended, or has the capability to cause death or serious bodily injury to a significant number of persons through the release, dissemination, or impact of toxic or poisonous chemicals or their precursors;

(3) any weapon involving a biological agent, toxin, or vector (as such terms are defined in section 178 of title 18, United States Code) that is designed, intended, or has the capability to cause death, illness, or serious bodily injury to a significant number of persons; or

(4) any weapon that is designed, intended, or has the capability to release radiation or radioactivity causing death, illness, or serious bodily injury to a significant number of persons.

**AUTHORIZATION FOR ELECTRONIC SURVEILLANCE
FOR FOREIGN INTELLIGENCE PURPOSES**

SEC. 102. [50 U.S.C. § 1802]

(a)(1) Notwithstanding any other law, the President, through the Attorney General, may authorize electronic surveillance without a court order under this title to acquire foreign intelligence information for periods of up to one year if the Attorney General certifies in writing under oath that—

(A) the electronic surveillance is solely directed at—

(i) the acquisition of the contents of communications transmitted by means of communications used exclusively between or among foreign powers, as defined in section 101(a)(1), (2), or (3); or

(ii) the acquisition of technical intelligence, other than the spoken communications of individuals, from property or premises under the open and exclusive control of a foreign power, as defined in section 101(a)(1), (2), or (3);

(B) there is no substantial likelihood that the surveillance will acquire the contents of any communications to which a United States person is a party; and

(C) the proposed minimization procedures with respect to such surveillance meet the definition of minimization procedures under section 101(h); and

if the Attorney General reports such minimization procedures and any changes thereto to the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence at least thirty days prior to their effective date, unless the Attorney General determines immediate action is required and notifies the committees immediately of such minimization procedures and the reason for their becoming effective immediately.

(2) An electronic surveillance authorized by this subsection may be conducted only in accordance with the Attorney General's certification and the minimization procedures adopted by him. The Attorney General shall assess compliance with such procedures and shall report such assessments to the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence under the provisions of section 108(a).

(3) The Attorney General shall immediately transmit under seal to the court established under section 103(a) a copy of his certification. Such certification shall be maintained under security measures established by

the Chief Justice with the concurrence of the Attorney General, in consultation with the Director of National Intelligence, and shall remain sealed unless—

- (A) an application for a court order with respect to the surveillance is made under sections 101(h)(4) and 104; or
- (B) the certification is necessary to determine the legality of the surveillance under section 106(f).

(4) With respect to electronic surveillance authorized by this subsection, the Attorney General may direct a specified communication common carrier to—

- (A) furnish all information, facilities, or technical assistance necessary to accomplish the electronic surveillance in such a manner as will protect its secrecy and produce a minimum of interference with the services that such carrier is providing its customers; and
- (B) maintain under security procedures approved by the Attorney General and the Director of National Intelligence any records concerning the surveillance or the aid furnished which such carrier wishes to retain.

The Government shall compensate, at the prevailing rate, such carrier for furnishing such aid.

(b) Applications for a court order under this title are authorized if the President has, by written authorization, empowered the Attorney General to approve applications to the court having jurisdiction under section 103, and a judge to whom an application is made may, notwithstanding any other law, grant an order, in conformity with section 105, approving electronic surveillance of a foreign power or an agent of a foreign power for the purpose of obtaining foreign intelligence information, except that the court shall not have jurisdiction to grant any order approving electronic surveillance directed solely as described in paragraph (1)(A) of subsection (a) unless such surveillance may involve the acquisition of communications of any United States person.

DESIGNATION OF JUDGES

SEC. 103. [50 U.S.C. § 1803]

(a)(1) The Chief Justice of the United States shall publicly designate 11 district court judges from at least seven of the United States judicial circuits of whom no fewer than 3 shall reside within 20 miles of the District of Columbia who shall constitute a court which shall have jurisdiction to hear applications for and grant orders approving electronic surveillance anywhere within the United States under the procedures set forth in this Act, except that no judge designated under this

subsection (except when sitting en banc under paragraph (2)) shall hear the same application for electronic surveillance under this Act which has been denied previously by another judge designated under this subsection. If any judge so designated denies an application for an order authorizing electronic surveillance under this Act, such judge shall provide immediately for the record a written statement of each reason for his decision and, on motion of the United States, the record shall be transmitted, under seal, to the court of review established in subsection (b).

(2)(A) The court established under this subsection may, on its own initiative, or upon the request of the Government in any proceeding or a party under section 501(f) or paragraph (4) or (5) of section 702(i), hold a hearing or rehearing, en banc, when ordered by a majority of the judges that constitute such court upon a determination that—

- (i) en banc consideration is necessary to secure or maintain uniformity of the court's decisions; or
- (ii) the proceeding involves a question of exceptional importance.

(B) Any authority granted by this Act to a judge of the court established under this subsection may be exercised by the court en banc. When exercising such authority, the court en banc shall comply with any requirements of this Act on the exercise of such authority.

(C) For purposes of this paragraph, the court en banc shall consist of all judges who constitute the court established under this subsection.

(b) The Chief Justice shall publicly designate three judges, one of whom shall be publicly designated as the presiding judge, from the United States district courts or courts of appeals who together shall comprise a court of review which shall have jurisdiction to review the denial of any application made under this Act. If such court determines that the application was properly denied, the court shall provide for the record a written statement of each reason for its decision and, on petition of the United States for a writ of certiorari, the record shall be transmitted under seal to the Supreme Court, which shall have jurisdiction to review such decision.

(c) Proceedings under this Act shall be conducted as expeditiously as possible, and hearings shall be transcribed. The record of proceedings under this Act, including applications made, transcriptions of hearings, and orders granted, shall be maintained under security measures established by the Chief Justice in consultation with the Attorney General and the Director of National Intelligence. Transcriptions and any related records, including testimony and affidavits, shall be stored in a file associated with the relevant application or order.

(d) Each judge designated under this section shall so serve for a maximum of seven years and shall not be eligible for redesignation, except that the judges first designated under subsection (a) shall be designated for terms of from one to seven years so that one term expires each year, and that judges first designated under subsection (b) shall be designated for terms of three, five, and seven years.

(e)(1) Three judges designated under subsection (a) who reside within 20 miles of the District of Columbia, or, if all of such judges are unavailable, other judges of the court established under subsection (a) as may be designated by the presiding judge of such court, shall comprise a petition review pool which shall have jurisdiction to review petitions filed pursuant to section 501(f)(1) or 702(i)(4).

(2) Not later than 60 days after March 9, 2006, the court established under subsection (a) shall adopt and, consistent with the protection of national security, publish procedures for the review of petitions filed pursuant to section 501(f)(1) or 702(i)(4) by the panel established under paragraph (1). Such procedures shall provide that review of a petition shall be conducted in camera and shall also provide for the designation of an acting presiding judge.

(f)(1) A judge of the court established under subsection (a), the court established under subsection (b) or a judge of that court, or the Supreme Court of the United States or a justice of that court, may, in accordance with the rules of their respective courts, enter a stay of an order or an order modifying an order of the court established under subsection (a) or the court established under subsection (b) entered under any title of this Act, while the court established under subsection (a) conducts a rehearing, while an appeal is pending to the court established under subsection (b), or while a petition of certiorari is pending in the Supreme Court of the United States, or during the pendency of any review by that court.

(2) The authority described in paragraph (1) shall apply to an order entered under any provision of this Act.

(g)(1) The courts established pursuant to subsections (a) and (b) may establish such rules and procedures, and take such actions, as are reasonably necessary to administer their responsibilities under this Act.

(2) The rules and procedures established under paragraph (1), and any modifications of such rules and procedures, shall be recorded, and shall be transmitted to the following:

(A) All of the judges on the court established pursuant to subsection (a).

(B) All of the judges on the court of review established pursuant to subsection (b).

(C) The Chief Justice of the United States.

- (D) The Committee on the Judiciary of the Senate.
- (E) The Select Committee on Intelligence of the Senate.
- (F) The Committee on the Judiciary of the House of Representatives.
- (G) The Permanent Select Committee on Intelligence of the House of Representatives.

(3) The transmissions required by paragraph (2) shall be submitted in unclassified form, but may include a classified annex.

(h) Nothing in this Act shall be construed to reduce or contravene the inherent authority of a court established under this section to determine or enforce compliance with an order or a rule of such court or with a procedure approved by such court.

(i) AMICUS CURIAE.—

(1) DESIGNATION.—The presiding judges of the courts established under subsections (a) and (b) shall, not later than 180 days after June 2, 2015, jointly designate not fewer than 5 individuals to be eligible to serve as amicus curiae, who shall serve pursuant to rules the presiding judges may establish. In designating such individuals, the presiding judges may consider individuals recommended by any source, including members of the Privacy and Civil Liberties Oversight Board, the judges determine appropriate.

(2) AUTHORIZATION.

(A) IN GENERAL - A court established under subsection (a) or (b), consistent with the requirement of subsection (c) and any other statutory requirement that the court act expeditiously or within a stated time—

(i) shall appoint one or more individuals who have been designated under paragraph (1) to serve as amicus curiae to assist such court in the consideration of any application for an order or review that, in the opinion of the court, presents a novel or significant interpretation of the law, unless the court issues a finding that such appointment is not appropriate;

(ii) may appoint one or more individuals or organizations to serve as amicus curiae, including to provide technical expertise, in any instance as such court deems appropriate or, upon motion, permit an individual or organization leave to file an amicus curiae brief;

(iii) shall appoint one or more individuals who have been designated under paragraph (1) to serve as amicus curiae to assist such court in the consideration of any

certification or procedures submitted for review pursuant to section 702, including any amendments to such certifications or procedures, if the court established under subsection (a) has not appointed an individual under clause (i) or (ii), unless the court issues a finding that such appointment is not appropriate or is likely to result in undue delay.

(B) EXPERTISE.—In appointing one or more individuals under subparagraph (A)(iii), the court shall, to the maximum extent practicable, appoint an individual who possesses expertise in both privacy and civil liberties and intelligence collection.

(C) TIMING.—In the event that the court appoints one or more individuals or organizations pursuant to this paragraph to assist such court in a proceeding under section 702, notwithstanding subsection (j)(1)(B) of such section, the court shall issue an order pursuant to subsection (j)(3) of such section as expeditiously as possible consistent with subsection (k)(1) of such section, but in no event later than 60 days after the date on which such certification, procedures, or amendments are submitted for the court's review, or later than 60 days after the court has issued an order appointing one or more individuals pursuant to this paragraph, whichever is earlier, unless a judge of that court issues an order finding that extraordinary circumstances necessitate additional time for review and that such extension of time is consistent with the national security.

(3) QUALIFICATIONS OF AMICUS CURIAE.—

(A) EXPERTISE.—Individuals designated under paragraph (1) shall be persons who possess expertise in privacy and civil liberties, intelligence collection, communications technology, or any other area that may lend legal or technical expertise to a court established under subsection (a) or (b).

(B) SECURITY CLEARANCE.—Individuals designated pursuant to paragraph (1) shall be persons who are determined to be eligible for access to classified information necessary to participate in matters before the courts. Amicus curiae appointed by the court pursuant to paragraph (2) shall be persons who are determined to be eligible for access to classified information, if such access is necessary to participate in the matters in which they may be appointed.

(4) DUTIES.—If a court established under subsection (a) or (b) appoints an amicus curiae under paragraph (2), the amicus curiae shall—

(A) be limited to addressing the specific issues identified by the court; and

(B) provide to the court, as appropriate—

(i) legal arguments that advance the protection of individual privacy and civil liberties of United States persons;

(ii) information related to intelligence collection or communications technology; or

(iii) legal arguments or information regarding any other area relevant to the issue presented to the court.

(5) ASSISTANCE.—An amicus curiae appointed under paragraph (2)(A) may request that the court designate or appoint additional amici curiae pursuant to paragraph (1) or paragraph (2), to be available to assist the amicus curiae.

(6) ACCESS TO INFORMATION.—

(A) IN GENERAL.—If a court established under subsection (a) or (b) appoints an amicus curiae under paragraph (2), the amicus curiae—

(i) shall have access to any legal precedent, application, certification, petition, motion, or such other materials that the court determines are relevant to the duties of the amicus curiae; and

(ii) may, if the court determines that it is relevant to the duties of the amicus curiae, consult with any other individuals designated pursuant to paragraph (1) regarding information relevant to any assigned proceeding.

(B) BRIEFINGS.—The Attorney General may periodically brief or provide relevant materials to individuals designated pursuant to paragraph (1) regarding constructions and interpretations of this Act and legal, technological, and other issues related to actions authorized by this Act.

(C) CLASSIFIED INFORMATION.—An amicus curiae designated or appointed by the court may have access to classified documents, information, and other materials or proceedings only if that individual is eligible for access to classified information and to the extent consistent with the national security of the United States.

(D) RULE OF CONSTRUCTION.—Nothing in this section shall be construed to require the Government to provide information to

an amicus curiae appointed by the court that is privileged from disclosure.

(7) NOTIFICATION.—A presiding judge of a court established under subsection (a) or (b) shall notify the Attorney General of each exercise of the authority to appoint an individual to serve as amicus curiae under paragraph (2).

(8) ASSISTANCE.—A court established under subsection (a) or (b) may request and receive (including on a nonreimbursable basis) the assistance of the executive branch in the implementation of this subsection.

(9) ADMINISTRATION.—A court established under subsection (a) or (b) may provide for the designation, appointment, removal, training, or other support for an individual designated to serve as amicus curiae under paragraph (1) or appointed to serve as amicus curiae under paragraph (2) in a manner that is not inconsistent with this subsection.

(10) RECEIPT OF INFORMATION.—Nothing in this subsection shall limit the ability of a court established under subsection (a) or (b) to request or receive information or materials from, or otherwise communicate with, the Government or amicus curiae appointed under paragraph (2) on an ex parte basis, nor limit any special or heightened obligation in any ex parte communication or proceeding.

(11) COMPENSATION.—Notwithstanding any other provision of law, a court established under subsection (a) or (b) may compensate an amicus curiae appointed under paragraph (2) for assistance provided under such paragraph as the court considers appropriate and at such rate as the court considers appropriate.

(j) REVIEW OF FISA COURT DECISIONS.—Following issuance of an order under this Act, a court established under subsection (a) shall certify for review to the court established under subsection (b) any question of law that may affect resolution of the matter in controversy that the court determines warrants such review because of a need for uniformity or because consideration by the court established under subsection (b) would serve the interests of justice. Upon certification of a question of law under this subsection, the court established under subsection (b) may give binding instructions or require the entire record to be sent up for decision of the entire matter in controversy.

(k) REVIEW OF FISA COURT OF REVIEW DECISIONS.—

(1) CERTIFICATION.—For purposes of section 1254(2) of Title 28, United States Code, the court of review established under subsection (b) shall be considered to be a court of appeals.

(2) AMICUS CURIAE BRIEFING.—Upon certification of an application under paragraph (1), the Supreme Court of the United States may appoint

an amicus curiae designated under subsection (i)(1), or any other person, to provide briefing or other assistance.

(l) DESIGNATION OF COUNSEL FOR CERTAIN APPLICATIONS.—To assist the court in the consideration of any application for an order pursuant to section 104 that targets a United States person, the presiding judge designated under subsection (a) shall designate one or more attorneys to review such applications, and provide a written analysis to the judge considering the application, of—

(1) the sufficiency of the evidence used to make the probable cause determination under section 105(a)(2);

(2) any material weaknesses, flaws, or other concerns in the application; and

(3) a recommendation as to the following, which the judge shall consider during a proceeding on the application in which such attorney is present, as appropriate—

(A) that the application should be approved, denied, or modified;

(B) that the Government should supply additional information in connection with such application; or

(C) that any requirements or conditions should be imposed on the Government for the approval of such application.

(m) REMOVAL OR SUSPENSION OF FEDERAL OFFICERS FOR MISCONDUCT BEFORE COURTS.—An officer or employee of the United States Government who engages in intentional misconduct with respect to proceedings before the Foreign Intelligence Surveillance Court or the Foreign Intelligence Surveillance Court of Review shall be subject to appropriate adverse actions, including, at minimum, suspension without pay or removal, up to and including termination.

APPLICATION FOR AN ORDER

SEC. 104. [50 U.S.C. § 1804]

(a) Each application for an order approving electronic surveillance under this title shall be made by a Federal officer in writing upon oath or affirmation to a judge having jurisdiction under section 103. Each application shall require the approval of the Attorney General based upon his finding that it satisfies the criteria and requirements of such application as set forth in this title. It shall include—

(1) the identity of the Federal officer making the application;

(2) the identity, if known, or a description of the specific target of the electronic surveillance;

(3) a sworn statement of the facts and circumstances relied upon by the applicant to justify his belief that—

(A) the target of the electronic surveillance is a foreign power or an agent of a foreign power, and, in the case of a target that is a

- United States person alleged to be acting as an agent of a foreign power (as described in section 101(b)(2)(B)), that a violation of the criminal statutes of the United States as referred to in section 101(b)(2)(B) has occurred or is about to occur; and
- (B) each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power;
- (4) a statement of the proposed minimization procedures;
- (5) a description of the nature of the information sought and the type of communications or activities to be subjected to the surveillance;
- (6) a certification or certifications by the Assistant to the President for National Security Affairs, an executive branch official or officials designated by the President from among those executive officers employed in the area of national security or defense and appointed by the President with the advice and consent of the Senate, or the Deputy Director of the Federal Bureau of Investigation, if designated by the President as a certifying official —
- (A) that the certifying official deems the information sought to be foreign intelligence information;
- (B) that a significant purpose of the surveillance is to obtain foreign intelligence information;
- (C) that such information cannot reasonably be obtained by normal investigative techniques;
- (D) that designates the type of foreign intelligence information being sought according to the categories described in section 101(e);
- (E) including a statement of the basis for the certification that—
- (i) the information sought is the type of foreign intelligence information designated; and
- (ii) such information cannot reasonably be obtained by normal investigative techniques; and
- (F) that none of the information included in the statement described in paragraph (3) was solely produced by, derived from information produced by, or obtained using the funds of, a political organization (as such term is defined in section 527 of the Internal Revenue Code of 1986), unless—
- (i) the political organization is clearly identified in the body of the statement described in paragraph (3);
- (ii) the information has been corroborated; and

- (iii) the investigative techniques used to corroborate the information are clearly identified in the body of the statement described in paragraph (3); and
- (G) that none of the information included in the statement described in paragraph (3) is attributable to or derived from the content of a media source unless the statement includes a clear identification of each author of that content, and where applicable, the publisher of that content, information to corroborate that which was derived from the media source, and an explanation of the investigative techniques used to corroborate the information;
- (7) a summary statement of the means by which the surveillance will be effected and a statement whether physical entry is required to effect the surveillance;
- (8) a statement of the facts concerning all previous applications that have been made to any judge under this title involving any of the persons, facilities, or places specified in the application, and the action taken on each previous application;
- (9) a statement of the period of time for which the electronic surveillance is required to be maintained, and if the nature of the intelligence gathering is such that the approval of the use of electronic surveillance under this title should not automatically terminate when the described type of information has first been obtained, a description of facts supporting the belief that additional information of the same type will be obtained thereafter; and
- (10) with respect to a target who is a United States person, a statement summarizing the investigative techniques carried out before making the application;
- (11) in the case of an application for an extension of an order under this title for a surveillance targeted against a United States person, a summary statement of the foreign intelligence information obtained pursuant to the original order (and any preceding extension thereof) as of the date of the application for the extension, or a reasonable explanation of the failure to obtain such information; and
- (12) a certification by the applicant or declarant that, to the best knowledge of the applicant or declarant, the Attorney General or a designated attorney for the Government has been apprised of all information that might reasonably—
 - (A) call into question the accuracy of the application or the reasonableness of any assessment in the application conducted

by the department or agency on whose behalf the application is made; or

(B) otherwise raise doubts with respect to the findings required under section 105(a).

(13) non-cumulative information known to the applicant or declarant that is potentially exculpatory regarding the requested legal findings or any assessment in the application.

(b) The Attorney General may require any other affidavit or certification from any other officer in connection with the application.

(c) The judge may require the applicant to furnish such other information as may be necessary to make the determinations required by section 105.

(d)(1)(A) Upon written request of the Director of the Federal Bureau of Investigation, the Secretary of Defense, the Secretary of State, or the Director of National Intelligence, or the Director of the Central Intelligence Agency, the Attorney General shall personally review under subsection (a) an application under that subsection for a target described in section 101(b)(2).

(B) Except when disabled or otherwise unavailable to make a request referred to in subparagraph (A), an official referred to in that subparagraph may not delegate the authority to make a request referred to in that subparagraph.

(C) Each official referred to in subparagraph (A) with authority to make a request under that subparagraph shall take appropriate actions in advance to ensure that delegation of such authority is clearly established in the event such official is disabled or otherwise unavailable to make such request.

(2)(A) If as a result of a request under paragraph (1) the Attorney General determines not to approve an application under the second sentence of subsection (a) for purposes of making the application under this section, the Attorney General shall provide written notice of the determination to the official making the request for the review of the application under that paragraph. Except when disabled or otherwise unavailable to make a determination under the preceding sentence, the Attorney General may not delegate the responsibility to make a determination under that sentence. The Attorney General shall take appropriate actions in advance to ensure that delegation of such responsibility is clearly established in the event the Attorney General is disabled or otherwise unavailable to make such determination.

(B) Notice with respect to an application under subparagraph (A) shall set forth the modifications, if any, of the application that are necessary in order for the Attorney General to approve the

application under the second sentence of subsection (a) for purposes of making the application under this section.

(C) Upon review of any modifications of an application set forth under subparagraph (B), the official notified of the modifications under this paragraph shall modify the application if such official determines that such modification is warranted. Such official shall supervise the making of any modification under this subparagraph. Except when disabled or otherwise unavailable to supervise the making of any modification under the preceding sentence, such official may not delegate the responsibility to supervise the making of any modification under that preceding sentence. Each such official shall take appropriate actions in advance to ensure that delegation of such responsibility is clearly established in the event such official is disabled or otherwise unavailable to supervise the making of such modification.

ISSUANCE OF AN ORDER

SEC. 105. [50 U.S.C. § 1805]

(a) Upon an application made pursuant to section 104, the judge shall enter an ex parte order as requested or as modified approving the electronic surveillance if he finds that—

(1) the application has been made by a Federal officer and approved by the Attorney General;

(2) on the basis of the facts submitted by the applicant there is probable cause to believe that—

(A) the target of the electronic surveillance is a foreign power or an agent of a foreign power: *Provided*, That no United States person may be considered a foreign power or an agent of a foreign power solely upon the basis of activities protected by the first amendment to the Constitution of the United States; and

(B) each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power;

(3) the proposed minimization procedures meet the definition of minimization procedures under section 101(h); and

(4) the application which has been filed contains all statements and certifications required by section 104 and, if the target is a United States person, the certification or certifications are not clearly erroneous on the basis of the statement made under section 104(a)(7)(E) and any other information furnished under section 104(d).

(b) In determining whether or not probable cause exists for purposes of an order under subsection (a)(2), a judge may consider past activities of the target, as well as facts and circumstances relating to current or future activities of the target.

(c)(1) SPECIFICATIONS.—An order approving an electronic surveillance under this section shall specify—

(A) the identity, if known, or a description of the specific target of the electronic surveillance identified or described in the application pursuant to section 104(a)(3);

(B) the nature and location of each of the facilities or places at which the electronic surveillance will be directed, if known;

(C) the type of information sought to be acquired and the type of communications or activities to be subjected to the surveillance;

(D) the means by which the electronic surveillance will be effected and whether physical entry will be used to effect the surveillance; and

(E) the period of time during which the electronic surveillance is approved.

(2) DIRECTIONS.— An order approving an electronic surveillance under this section shall direct—

(A) that the minimization procedures be followed;

(B) that, upon the request of the applicant, a specified communication or other common carrier, landlord, custodian, or other specified person, furnish the applicant forthwith all information, facilities, or technical assistance necessary to accomplish the electronic surveillance in such a manner as will protect its secrecy and produce a minimum of interference with the services that such carrier, landlord, custodian, or other person is providing that target of electronic surveillance;

(C) that such carrier, landlord, custodian, or other person maintain under security procedures approved by the Attorney General and the Director of National Intelligence any records concerning the surveillance or the aid furnished that such person wishes to retain; and

(D) that the applicant compensate, at the prevailing rate, such carrier, landlord, custodian, or other person for furnishing such aid.

(3) SPECIAL DIRECTIONS FOR CERTAIN ORDERS.—An order approving an electronic surveillance under this section in circumstances where the nature and location of each of the facilities or places at which the surveillance will be directed is unknown shall direct the applicant to provide notice to the court within ten days after the date on which

surveillance begins to be directed at any new facility or place, unless the court finds good cause to justify a longer period of up to 60 days, of—

(A) the nature and location of each new facility or place at which the electronic surveillance is directed;

(B) the facts and circumstances relied upon by the applicant to justify the applicant's belief that each new facility or place at which the electronic surveillance is directed is or was being used, or is about to be used, by the target of the surveillance;

(C) a statement of any proposed minimization procedures that differ from those contained in the original application or order, that may be necessitated by a change in the facility or place at which the electronic surveillance is directed; and

(D) the total number of electronic surveillances that have been or are being conducted under the authority of the order.

(d)(1) An order issued under this section may approve an electronic surveillance for the period necessary to achieve its purpose, or for ninety days, whichever is less, except that

(A) an order under this section shall approve an electronic surveillance targeted against a foreign power, for the period specified in the application or for one year, whichever is less, and

(B) an order under this Act for a surveillance targeted against an agent of a foreign power who is not a United States person may be for the period specified in the application or for one year, whichever is less.

(2) At or before the end of the period of time for which electronic surveillance is approved by an order or an extension, the judge may assess compliance with the minimization procedures by reviewing the circumstances under which information concerning United States persons was acquired, retained, or disseminated.

(3) A denial of the application made under section 104 may be reviewed as provided in section 103.

(5) An extension of an order issued under this title for surveillance targeted against a United States person, to the extent practicable and absent exigent circumstances, shall be granted or denied by the same judge who issued the original order unless the term of such judge has expired or such judge is otherwise no longer serving on the court.

(e)(1) Notwithstanding any other provision of this title, the Attorney General may authorize the emergency employment of electronic surveillance if the Attorney General—

- (A) reasonably determines that an emergency situation exists with respect to the employment of electronic surveillance to obtain foreign intelligence information before an order authorizing such surveillance can with due diligence be obtained;
 - (B) reasonably determines that the factual basis for the issuance of an order under this title to approve such electronic surveillance exists;
 - (C) informs, either personally or through a designee, a judge having jurisdiction under section 103 at the time of such authorization that the decision has been made to employ emergency electronic surveillance; and
 - (D) makes an application in accordance with this title to a judge having jurisdiction under section 103 as soon as practicable, but not later than 7 days after the Attorney General authorizes such surveillance.
- (2) If the Attorney General authorizes the emergency employment of electronic surveillance under paragraph (1), the Attorney General shall require that the minimization procedures required by this title for the issuance of a judicial order be followed.
- (3) In the absence of a judicial order approving such electronic surveillance, the surveillance shall terminate when the information sought is obtained, when the application for the order is denied, or after the expiration of 7 days from the time of authorization by the Attorney General, whichever is earliest.
- (4) A denial of the application made under this subsection may be reviewed as provided in section 103.
- (5) In the event that such application for approval is denied, or in any other case where the electronic surveillance is terminated and no order is issued approving the surveillance, no information obtained or evidence derived from such surveillance shall be received in evidence or otherwise disclosed in any trial, hearing, or other proceeding in or before any court, grand jury, department, office, agency, regulatory body, legislative committee, or other authority of the United States, a State, or political subdivision thereof, and no information concerning any United States person acquired from such surveillance shall subsequently be used or disclosed in any other manner by Federal officers or employees without the consent of such person, except with the approval of the Attorney General if the information indicates a threat of death or serious bodily harm to any person.
- (6) The Attorney General shall assess compliance with the requirements of paragraph (5).

(f)(1) Notwithstanding any other provision of this Act, the lawfully authorized targeting of a non-United States person previously believed to be located outside the United States for the acquisition of foreign intelligence information may continue for a period not to exceed 72 hours from the time that the non-United States person is reasonably believed to be located inside the United States and the acquisition is subject to this title or to title III of this Act, provided that the head of an element of the intelligence community—

(A) reasonably determines that a lapse in the targeting of such non-United States person poses a threat of death or serious bodily harm to any person;

(B) promptly notifies the Attorney General of a determination under subparagraph (A); and

(C) requests, as soon as practicable, the employment of emergency electronic surveillance under subsection (e) or the employment of an emergency physical search pursuant to section 304(e), as warranted.

(2) The authority under this subsection to continue the acquisition of foreign intelligence information is limited to a period not to exceed 72 hours and shall cease upon the earlier of the following:

(A) The employment of emergency electronic surveillance under subsection (e) or the employment of an emergency physical search pursuant to section 304(e).

(B) An issuance of a court order under this title or title III of this Act.

(C) The Attorney General provides direction that the acquisition be terminated.

(D) The head of the element of the intelligence community conducting the acquisition determines that a request under paragraph (1)(C) is not warranted.

(E) When the threat of death or serious bodily harm to any person is no longer reasonably believed to exist.

(3) Nonpublicly available information concerning unconsenting United States persons acquired under this subsection shall not be disseminated during the 72 hour time period under paragraph (1) unless necessary to investigate, reduce, or eliminate the threat of death or serious bodily harm to any person.

(4) If the Attorney General declines to authorize the employment of emergency electronic surveillance under subsection (e) or the employment of an emergency physical search pursuant to section 304(e), or a court order is not obtained under this title or title III of this Act, information obtained during the 72 hour acquisition time period under

paragraph (1) shall not be retained, except with the approval of the Attorney General if the information indicates a threat of death or serious bodily harm to any person.

(5) Paragraphs (5) and (6) of subsection (e) shall apply to this subsection.

(g) Notwithstanding any other provision of this title, officers, employees, or agents of the United States are authorized in the normal course of their official duties to conduct electronic surveillance not targeted against the communications of any particular person or persons, under procedures approved by the Attorney General, solely to—

(1) test the capability of electronic equipment, if—

(A) it is not reasonable to obtain the consent of the persons incidentally subjected to the surveillance;

(B) the test is limited in extent and duration to that necessary to determine the capability of the equipment;

(C) the contents of any communication acquired are retained and used only for the purpose of determining the capability of the equipment, are disclosed only to test personnel, and are destroyed before or immediately upon completion of the test; and:

(D) *Provided*, That the test may exceed ninety days only with the prior approval of the Attorney General;

(2) determine the existence and capability of electronic surveillance equipment being used by persons not authorized to conduct electronic surveillance, if—

(A) it is not reasonable to obtain the consent of persons incidentally subjected to the surveillance;

(B) such electronic surveillance is limited in extent and duration to that necessary to determine the existence and capability of such equipment; and

(C) any information acquired by such surveillance is used only to enforce chapter 119 of title 18, United States Code, or section 705 of the Communications Act of 1934, or to protect information from unauthorized surveillance; or

(3) train intelligence personnel in the use of electronic surveillance equipment, if—

(A) it is not reasonable to—

(i) obtain the consent of the persons incidentally subjected to the surveillance;

(ii) train persons in the course of surveillances otherwise authorized by this title; or

(iii) train persons in the use of such equipment without engaging in electronic surveillance;

(B) such electronic surveillance is limited in extent and duration to that necessary to train the personnel in the use of the equipment; and

(C) no contents of any communication acquired are retained or disseminated for any purpose, but are destroyed as soon as reasonably possible.

(h) Certifications made by the Attorney General pursuant to section 102(a) and applications made and orders granted under this title shall be retained for a period of at least ten years from the date of the certification or application.

(i) No cause of action shall lie in any court against any provider of a wire or electronic communication service, landlord, custodian, or other person (including any officer, employee, agent, or other specified person thereof) that furnishes any information, facilities, or technical assistance in accordance with a court order or request for emergency assistance under this Act for electronic surveillance or physical search.

(j) In any case in which the Government makes an application to a judge under this title to conduct electronic surveillance involving communications and the judge grants such application, upon the request of the applicant, the judge shall also authorize the installation and use of pen registers and trap and trace devices, and direct the disclosure of the information set forth in section 402(d)(2).

USE OF INFORMATION

SEC. 106. [50 U.S.C. § 1806]

(a) Information acquired from an electronic surveillance conducted pursuant to this title concerning any United States person may be used and disclosed by Federal officers and employees without the consent of the United States person only in accordance with the minimization procedures required by this title. No otherwise privileged communication obtained in accordance with, or in violation of, the provisions of this Act shall lose its privileged character. No information acquired from an electronic surveillance pursuant to this title may be used or disclosed by Federal officers or employees except for lawful purposes.

(b) No information acquired pursuant to this title shall be disclosed for law enforcement purposes unless such disclosure is accompanied by a statement that such information, or any information derived therefrom, may only be used in a criminal proceeding with the advance authorization of the Attorney General.

(c) Whenever the Government intends to enter into evidence or otherwise use or disclose in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United

States, against an aggrieved person, any information obtained or derived from an electronic surveillance of that aggrieved person pursuant to the authority of this Act, the Government shall, prior to the trial, hearing, or other proceeding or at a reasonable time prior to an effort to so disclose or so use that information or submit it in evidence, notify the aggrieved person and the court or other authority in which the information is to be disclosed or used that the Government intends to so disclose or so use such information.

(d) Whenever any State or political subdivision thereof intends to enter into evidence or otherwise use or disclose in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of a State or a political subdivision thereof, against an aggrieved person any information obtained or derived from an electronic surveillance of that aggrieved person pursuant to the authority of this Act, the State or political subdivision thereof shall notify the aggrieved person, the court or other authority in which the information is to be disclosed or used, and the Attorney General that the State or political subdivision thereof intends to so disclose or so use such information.

(e) Any person against whom evidence obtained or derived from an electronic surveillance to which he is an aggrieved person is to be, or has been, introduced or otherwise used or disclosed in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, a State, or a political subdivision thereof, may move to suppress the evidence obtained or derived from such electronic surveillance on the grounds that—

- (1) the information was unlawfully acquired; or
- (2) the surveillance was not made in conformity with an order of authorization or approval.

Such a motion shall be made before the trial, hearing, or other proceeding unless there was no opportunity to make such a motion or the person was not aware of the grounds of the motion.

(f) Whenever a court or other authority is notified pursuant to subsection (c) or (d), or whenever a motion is made pursuant to subsection (e), or whenever any motion or request is made by an aggrieved person pursuant to any other statute or rule of the United States or any State before any court or other authority of the United States or any State to discover or obtain applications or orders or other materials relating to electronic surveillance or to discover, obtain, or suppress evidence or information obtained or derived from electronic surveillance under this Act, the United States district court or, where the motion is made before another authority, the United States district court in the same district as the authority, shall, notwithstanding any other law, if the Attorney General files an affidavit under oath that disclosure or an adversary hearing would harm the

national security of the United States, review in camera and ex parte the application, order, and such other materials relating to the surveillance as may be necessary to determine whether the surveillance of the aggrieved person was lawfully authorized and conducted. In making this determination, the court may disclose to the aggrieved person, under appropriate security procedures and protective orders, portions of the application, order, or other materials relating to the surveillance only where such disclosure is necessary to make an accurate determination of the legality of the surveillance.

(g) If the United States district court pursuant to subsection (f) determines that the surveillance was not lawfully authorized or conducted, it shall, in accordance with the requirements of law, suppress the evidence which was unlawfully obtained or derived from electronic surveillance of the aggrieved person or otherwise grant the motion of the aggrieved person. If the court determines that the surveillance was lawfully authorized and conducted, it shall deny the motion of the aggrieved person except to the extent that due process requires discovery or disclosure.

(h) Orders granting motions or requests under subsection (g), decisions under this section that electronic surveillance was not lawfully authorized or conducted, and orders of the United States district court requiring review or granting disclosure of applications, orders, or other materials relating to a surveillance shall be final orders and binding upon all courts of the United States and the several States except a United States court of appeals and the Supreme Court.

(i) In circumstances involving the unintentional acquisition by an electronic, mechanical, or other surveillance device of the contents of any communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are located within the United States, such contents shall be destroyed upon recognition, unless the Attorney General determines that the contents indicates a threat of death or serious bodily harm to any person.

(j) If an emergency employment of electronic surveillance is authorized under subsection (e) or (f) of section 105 and a subsequent order approving the surveillance is not obtained, the judge shall cause to be served on any United States person named in the application and on such other United States persons subject to electronic surveillance as the judge may determine in his discretion it is in the interest of justice to serve, notice of—

(1) the fact of the application;

(2) the period of the surveillance; and

(3) the fact that during the period information was or was not obtained.

On an ex parte showing of good cause to the judge the serving of the notice required by this subsection may be postponed or suspended for a period not to

exceed ninety days. Thereafter, on a further ex parte showing of good cause, the court shall forego ordering the serving of the notice required under this subsection.

(k)(1) Federal officers who conduct electronic surveillance to acquire foreign intelligence information under this title may consult with Federal law enforcement officers or law enforcement personnel of a State or political subdivision of a State (including the chief executive officer of that State or political subdivision who has the authority to appoint or direct the chief law enforcement officer of that State or political subdivision) to coordinate efforts to investigate or protect against—

(A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;

(B) sabotage, international terrorism, or the international proliferation of weapons of mass destruction by a foreign power or an agent of a foreign power; or

(C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power.

(2) Coordination authorized under paragraph (1) shall not preclude the certification required by section 104(a)(7)(B) or the entry of an order under section 105.

REPORT OF ELECTRONIC SURVEILLANCE

SEC. 107. [50 U.S.C. § 1807]

(a) ANNUAL REPORT.—In April of each year, the Attorney General shall transmit to the Administrative Office of the United States Courts and to the congressional intelligence committees and the Committees on the Judiciary of the House of Representatives and the Senate a report setting forth with respect to the preceding calendar year—

(1) the total number of applications made for orders and extensions of orders approving electronic surveillance under this title;

(2) the total number of such orders and extensions either granted, modified, or denied; and

(3) the total number of subjects targeted by electronic surveillance conducted under an order or emergency authorization under this title, rounded to the nearest 500, including the number of such individuals who are United States persons, reported to the nearest band of 500, starting with 0-499.

(b) FORM.—Each report under subsection (a) shall be submitted in unclassified form, to the extent consistent with national security. Not later than 7 days after the date on which the Attorney General submits each such report, the Attorney

General shall make the report publicly available, or, if the Attorney General determines that the report cannot be made publicly available consistent with national security, the Attorney General may make publicly available an unclassified summary of the report or a redacted version of the report.

CONGRESSIONAL OVERSIGHT

SEC. 108. [50 U.S.C. § 1808]

(a)(1) On a semiannual basis the Attorney General shall fully inform the Permanent Select Committee on Intelligence and the Committee on the Judiciary of the House of Representatives and the Select Committee on Intelligence and the Committee on the Judiciary of the Senate concerning all electronic surveillance under this title. Nothing in this title shall be deemed to limit the authority and responsibility of the appropriate committees of each House of Congress to obtain such information as they may need to carry out their respective functions and duties.

(2) Each report under the first sentence of paragraph (1) shall include a description of—

- (A) the total number of applications made for orders and extensions of orders approving electronic surveillance under this title where the nature and location of each facility or place at which the electronic surveillance will be directed is unknown;
- (B) each criminal case in which information acquired under this Act has been authorized for use at trial during the period covered by such report;
- (C) the total number of emergency employments of electronic surveillance under section 105(e) and the total number of subsequent orders approving or denying such electronic surveillance; and
- (D) the total number of authorizations under section 105(f) and the total number of subsequent emergency employments of electronic surveillance under section 105(e) or emergency physical searches pursuant to section 301(e).

(b) On or before one year after the effective date of this Act and on the same day each year for four years thereafter, the Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence shall report respectively to the House of Representatives and the Senate, concerning the implementation of this Act. Said reports shall include but not be limited to an analysis and recommendations concerning whether this Act should be (1) amended, (2) repealed, or (3) permitted to continue in effect without amendment.

PENALTIES

SEC. 109. [50 U.S.C. § 1809]

(a) OFFENSE.—A person is guilty of an offense if he—

(1) intentionally engages in electronic surveillance under color of law except as authorized by this Act, chapter 119, 121, or 206 of title 18, United States Code, or any express statutory authorization that is an additional exclusive means for conducting electronic surveillance under section 112;

(2) intentionally discloses or uses information obtained under color of law by electronic surveillance, knowing or having reason to know that the information was obtained through electronic surveillance not authorized by this Act, chapter 119, 121, or 206 of title 18, United States Code, or any express statutory authorization that is an additional exclusive means for conducting electronic surveillance under section 112; or

(3) knowingly and willfully communicates, furnishes, transmits, or otherwise makes available to an unauthorized person, or publishes, or uses in any manner prejudicial to the safety or interest of the United States or for the benefit of any foreign government to the detriment of the United States an application, in whole or in part, for an order for electronic surveillance under this Act.

(b) DEFENSE.—It is a defense to a prosecution under paragraph (1) or (2) of subsection (a) that the defendant was a law enforcement or investigative officer engaged in the course of his official duties and the electronic surveillance was authorized by and conducted pursuant to a search warrant or court order of a court of competent jurisdiction.

(c) PENALTY.—A person guilty of an offense in this section shall be fined under title 18, imprisoned for not more than 10 years, or both.

(d) JURISDICTION.—There is Federal jurisdiction over an offense under this section if the person committing the offense was an officer or employee of the United States at the time the offense was committed.

CIVIL LIABILITY

SEC. 110. [50 U.S.C. § 1810]

An aggrieved person, other than a foreign power or an agent of a foreign power, as defined in section 101 (a) or (b)(1)(A), respectively, who has been subjected to an electronic surveillance or about whom information obtained by electronic surveillance of such person has been disclosed or used in violation of section 109

shall have a cause of action against any person who committed such violation and shall be entitled to recover—

(a) actual damages, but not less than liquidated damages equal to the greater of—

(1) if the aggrieved person is a United States person, \$10,000 or \$1,000 per day for each day of violation; or

(2) for any other aggrieved person, \$1,000 or \$100 per day for each day of violation;

(b) punitive damages; and

(c) reasonable attorney's fees and other investigation and litigation costs reasonably incurred.

REPORTING REQUIREMENTS FOR CIVIL ACTIONS.

SEC. 110A. [50 U.S.C. § 1810A]

(a) **REPORT TO CONGRESS.**—If a court finds that a person has violated this Act in a civil action under section 110, the head of the agency that employs that person shall report to Congress on the administrative action taken against that person pursuant to section 103(m) or any other provision of law.

(b) **REPORT TO FOREIGN INTELLIGENCE SURVEILLANCE COURT.**— If a court finds that a person has violated this Act in a civil action under section 110, the head of the agency that employs that person shall report the name of such person to the Foreign Intelligence Surveillance Court. The Foreign Intelligence Surveillance Court shall maintain a list of each person about whom it received a report under this subsection.

AUTHORIZATION DURING TIME OF WAR

SEC. 111. [50 U.S.C. § 1811]

Notwithstanding any other law, the President, through the Attorney General, may authorize electronic surveillance without a court order under this title to acquire foreign intelligence information for a period not to exceed fifteen calendar days following a declaration of war by the Congress.

STATEMENT OF EXCLUSIVE MEANS BY WHICH ELECTRONIC SURVEILLANCE AND INTERCEPTION OF CERTAIN COMMUNICATIONS MAY BE CONDUCTED

SEC. 112. [50 U.S.C. § 1812]

(a) Except as provided in subsection (b), the procedures of chapters 119, 121, and 206 of title 18, United States Code, and this Act shall be the exclusive means by

which electronic surveillance and the interception of domestic wire, oral, or electronic communications may be conducted.

(b) Only an express statutory authorization for electronic surveillance or the interception of domestic wire, oral, or electronic communications, other than as an amendment to this Act or chapters 119, 121, or 206 of title 18, United States Code, shall constitute an additional exclusive means for the purpose of subsection (a).

TITLE II—CONFORMING AMENDMENTS

[SEC. 201. Amended Title 18.]

TITLE III—PHYSICAL SEARCHES WITHIN THE UNITED STATES FOR FOREIGN INTELLIGENCE PURPOSES

DEFINITIONS

SEC. 301. [50 U.S.C. § 1821]

As used in this title:

- (1) The terms “foreign power”, “agent of a foreign power”, “international terrorism”, “sabotage”, “foreign intelligence information”, “Attorney General”, “United States person”, “United States,” “person,” “weapon of mass destruction”, and “State” shall have the same meanings as in section 101 of this Act, except as specifically provided by this title.
- (2) “Aggrieved person” means a person whose premises, property, information, or material is the target of physical search or any other person whose premises, property, information, or material was subject to physical search.
- (3) “Foreign Intelligence Surveillance Court” means the court established by section 103(a) of this Act.
- (4) “Minimization procedures” with respect to physical search, means—
 - (A) specific procedures, which shall be adopted by the Attorney General, that are reasonably designed in light of the purposes and technique of the particular physical search, to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information;
 - (B) procedures that require that nonpublicly available information, which is not foreign intelligence information, as defined in section 101(e)(1) of this Act, shall not be disseminated in a manner that identifies any United States person, without such person’s consent, unless such person’s

identity is necessary to understand such foreign intelligence information or assess its importance;

(C) notwithstanding subparagraphs (A) and (B), procedures that allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes; and

(D) notwithstanding subparagraphs (A), (B), and (C), with respect to any physical search approved pursuant to section 302(a), procedures that require that no information, material, or property of a United States person shall be disclosed, disseminated, or used for any purpose or retained for longer than 72 hours unless a court order under section 304 is obtained or unless the Attorney General determines that the information indicates a threat of death or serious bodily harm to any person.

(5) “Physical search” means any physical intrusion within the United States into premises or property (including examination of the interior of property by technical means) that is intended to result in a seizure, reproduction, inspection, or alteration of information, material, or property, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, but does not include (A) “electronic surveillance”, as defined in section 101(f) of this Act, or (B) the acquisition by the United States Government of foreign intelligence information from international or foreign communications, or foreign intelligence activities conducted in accordance with otherwise applicable Federal law involving a foreign electronic communications system, utilizing a means other than electronic surveillance as defined in section 101(f) of this Act.

AUTHORIZATION OF PHYSICAL SEARCHES FOR FOREIGN INTELLIGENCE PURPOSES

SEC. 302. [50 U.S.C. § 1822]

(a)(1) Notwithstanding any other provision of law, the President, acting through the Attorney General, may authorize physical searches without a court order under this title to acquire foreign intelligence information for periods of up to one year if—

- (A) the Attorney General certifies in writing under oath that—
 - (i) the physical search is solely directed at premises, information, material, or property used exclusively by, or under the open and exclusive control of, a foreign power or powers (as defined in section 101(a)(1), (2), or (3));

- (ii) there is no substantial likelihood that the physical search will involve the premises, information, material, or property of a United States person; and
 - (iii) the proposed minimization procedures with respect to such physical search meet the definition of minimization procedures under subparagraphs (A) through (D) of section 301(4); and
 - (B) the Attorney General reports such minimization procedures and any changes thereto to the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate at least 30 days before their effective date, unless the Attorney General determines that immediate action is required and notifies the committees immediately of such minimization procedures and the reason for their becoming effective immediately.
- (2) A physical search authorized by this subsection may be conducted only in accordance with the certification and minimization procedures adopted by the Attorney General. The Attorney General shall assess compliance with such procedures and shall report such assessments to the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate under the provisions of section 306.
- (3) The Attorney General shall immediately transmit under seal to the Foreign Intelligence Surveillance Court a copy of the certification. Such certification shall be maintained under security measures established by the Chief Justice of the United States with the concurrence of the Attorney General, in consultation with the Director of National Intelligence, and shall remain sealed unless—
- (A) an application for a court order with respect to the physical search is made under section 301(4) and section 303; or
 - (B) the certification is necessary to determine the legality of the physical search under section 305(g).
- (4)(A) With respect to physical searches authorized by this subsection, the Attorney General may direct a specified landlord, custodian, or other specified person to—
- (i) furnish all information, facilities, or assistance necessary to accomplish the physical search in such a manner as will protect its secrecy and produce a minimum of interference with the services that such landlord, custodian, or other person is providing the target of the physical search; and

(ii) maintain under security procedures approved by the Attorney General and the Director of National Intelligence any records concerning the search or the aid furnished that such person wishes to retain.

(B) The Government shall compensate, at the prevailing rate, such landlord, custodian, or other person for furnishing such aid.

(b) Applications for a court order under this title are authorized if the President has, by written authorization, empowered the Attorney General to approve applications to the Foreign Intelligence Surveillance Court. Notwithstanding any other provision of law, a judge of the court to whom application is made may grant an order in accordance with section 304 approving a physical search in the United States of the premises, property, information, or material of a foreign power or an agent of a foreign power for the purpose of collecting foreign intelligence information.

(c) The Foreign Intelligence Surveillance Court shall have jurisdiction to hear applications for and grant orders approving a physical search for the purpose of obtaining foreign intelligence information anywhere within the United States under the procedures set forth in this title, except that no judge (except when sitting en banc) shall hear the same application which has been denied previously by another judge designated under section 103(a) of this Act. If any judge so designated denies an application for an order authorizing a physical search under this title, such judge shall provide immediately for the record a written statement of each reason for such decision and, on motion of the United States, the record shall be transmitted, under seal, to the court of review established under section 103(b).

(d) The court of review established under section 103(b) shall have jurisdiction to review the denial of any application made under this title. If such court determines that the application was properly denied, the court shall provide for the record a written statement of each reason for its decision and, on petition of the United States for a writ of certiorari, the record shall be transmitted under seal to the Supreme Court, which shall have jurisdiction to review such decision.

(e) Judicial proceedings under this title shall be concluded as expeditiously as possible. The record of proceedings under this title, including applications made and orders granted, shall be maintained under security measures established by the Chief Justice of the United States in consultation with the Attorney General and the Director of National Intelligence.

APPLICATION FOR AN ORDER

SEC. 303. [50 U.S.C. § 1823]

(a) Each application for an order approving a physical search under this title shall be made by a Federal officer in writing upon oath or affirmation to a judge of the Foreign Intelligence Surveillance Court. Each application shall require the approval of the Attorney General based upon the Attorney General's finding that it satisfies the criteria and requirements for such application as set forth in this title. Each application shall include—

- (1) the identity of the Federal officer making the application;
- (2) the identity, if known, or a description of the target of the search, and a description of the premises or property to be searched and of the information, material, or property to be seized, reproduced, or altered;
- (3) a sworn statement of the facts and circumstances relied upon by the applicant to justify the applicant's belief that—
 - (A) the target of the physical search is a foreign power or an agent of a foreign power. and, in the case of a target that is a United States person alleged to be acting as an agent of a foreign power (as described in section 101(b)(2)(B)), that a violation of the criminal statutes of the United States as referred to in section 101(b)(2)(B) has occurred or is about to occur;
 - (B) the premises or property to be searched contains foreign intelligence information; and
 - (C) the premises or property to be searched is or is about to be owned, used, possessed by, or is in transit to or from a foreign power or an agent of a foreign power;
- (4) a statement of the proposed minimization procedures;
- (5) a statement of the nature of the foreign intelligence sought and the manner in which the physical search is to be conducted;
- (6) a certification or certifications by the Assistant to the President for National Security Affairs, an executive branch official or officials designated by the President from among those executive branch officers employed in the area of national security or defense and appointed by the President, by and with the advice and consent of the Senate, or the Deputy Director of the Federal Bureau of Investigation, if designated by the President as a certifying official—
 - (A) that the certifying official deems the information sought to be foreign intelligence information;
 - (B) that a significant purpose of the search is to obtain foreign intelligence information;

- (C) that such information cannot reasonably be obtained by normal investigative techniques;
 - (D) that designates the type of foreign intelligence information being sought according to the categories described in section 101(e);
 - (E) includes a statement explaining the basis for the certifications required by subparagraphs (C) and (D); and
 - (F) that none of the information included in the statement described in paragraph (3) was solely produced by, derived from information produced by, or obtained using the funds of, a political organization (as such term is defined in section 527 of the Internal Revenue Code of 1986), unless—
 - (i) the political organization is clearly identified in the body of the statement described in paragraph (3);
 - (ii) the information has been corroborated; and
 - (iii) the investigative techniques used to corroborate the information are clearly identified in the body of the statement described in paragraph (3); and
 - (G) that none of the information included in the statement described in paragraph (3) is attributable to or derived from the content of a media source unless the statement includes a clear identification of each author of that content, where applicable, the publisher of that content, information to corroborate that which was derived from the media source, and an explanation of the investigative techniques used to corroborate the information;
- (7) where the physical search involves a search of the residence of a United States person, the Attorney General shall state what investigative techniques have previously been utilized to obtain the foreign intelligence information concerned and the degree to which these techniques resulted in acquiring such information;
- (8) a statement of the facts concerning all previous applications that have been made to any judge under this title involving any of the persons, premises, or property specified in the application, and the action taken on each previous application;
- (9) in the case of an application for an extension of an order under this title in which the target of the physical search is a United States person, a summary statement of the foreign intelligence information obtained pursuant to the original order (and any preceding extension thereof) as of the date of the application for the extension, or a reasonable explanation of the failure to obtain such information; and

(10) a certification by the applicant that, to the best knowledge of the applicant, the Attorney General or a designated attorney for the Government has been apprised of all information that might reasonably—

(A) call into question the accuracy of the application or the reasonableness of any assessment in the application conducted by the department or agency on whose behalf the application is made; or

(B) otherwise raise doubts with respect to the findings required under section 304(a).

(b) The Attorney General may require any other affidavit or certification from any other officer in connection with the application.

(c) The judge may require the applicant to furnish such other information as may be necessary to make the determinations required by section 304.

(d)(1)(A) Upon written request of the Director of the Federal Bureau of Investigation, the Secretary of Defense, the Secretary of State, the Director of National Intelligence, or the Director of the Central Intelligence Agency, the Attorney General shall personally review under subsection (a) an application under that subsection for a target described in section 101(b)(2).

(B) Except when disabled or otherwise unavailable to make a request referred to in subparagraph (A), an official referred to in that subparagraph may not delegate the authority to make a request referred to in that subparagraph.

(C) Each official referred to in subparagraph (A) with authority to make a request under that subparagraph shall take appropriate actions in advance to ensure that delegation of such authority is clearly established in the event such official is disabled or otherwise unavailable to make such request.

(2)(A) If as a result of a request under paragraph (1) the Attorney General determines not to approve an application under the second sentence of subsection (a) for purposes of making the application under this section, the Attorney General shall provide written notice of the determination to the official making the request for the review of the application under that paragraph. Except when disabled or otherwise unavailable to make a determination under the preceding sentence, the Attorney General may not delegate the responsibility to make a determination under that sentence. The Attorney General shall take appropriate actions in advance to ensure that delegation of such responsibility is clearly established in the event the Attorney General is disabled or otherwise unavailable to make such determination.

(B) Notice with respect to an application under subparagraph (A) shall set forth the modifications, if any, of the application that are necessary in order for the Attorney General to approve the application under the second sentence of subsection (a) for purposes of making the application under this section.

(C) Upon review of any modifications of an application set forth under subparagraph (B), the official notified of the modifications under this paragraph shall modify the application if such official determines that such modification is warranted. Such official shall supervise the making of any modification under this subparagraph. Except when disabled or otherwise unavailable to supervise the making of any modification under the preceding sentence, such official may not delegate the responsibility to supervise the making of any modification under that preceding sentence. Each such official shall take appropriate actions in advance to ensure that delegation of such responsibility is clearly established in the event such official is disabled or otherwise unavailable to supervise the making of such modification.

ISSUANCE OF AN ORDER

SEC. 304. [50 U.S.C. § 1824]

(a) Upon an application made pursuant to section 303, the judge shall enter an ex parte order as requested or as modified approving the physical search if the judge finds that—

(1) the application has been made by a Federal officer and approved by the Attorney General;

(2) on the basis of the facts submitted by the applicant there is probable cause to believe that—

(A) the target of the physical search is a foreign power or an agent of a foreign power, except that no United States person may be considered an agent of a foreign power solely upon the basis of activities protected by the first amendment to the Constitution of the United States; and

(B) the premises or property to be searched is or is about to be owned, used, possessed by, or is in transit to or from an agent of a foreign power or a foreign power;

(3) the proposed minimization procedures meet the definition of minimization contained in this title; and

(4) the application which has been filed contains all statements and certifications required by section 303, and, if the target is a United States

person, the certification or certifications are not clearly erroneous on the basis of the statement made under section 303(a)(6)(E) and any other information furnished under section 303(c).

(b) In determining whether or not probable cause exists for purposes of an order under subsection (a)(2), a judge may consider past activities of the target, as well as facts and circumstances relating to current or future activities of the target.

(c) An order approving a physical search under this section shall—

(1) specify—

(A) the identity, if known, or a description of the target of the physical search;

(B) the nature and location of each of the premises or property to be searched;

(C) the type of information, material, or property to be seized, altered, or reproduced;

(D) a statement of the manner in which the physical search is to be conducted and, whenever more than one physical search is authorized under the order, the authorized scope of each search and what minimization procedures shall apply to the information acquired by each search; and

(E) the period of time during which physical searches are approved; and

(2) direct—

(A) that the minimization procedures be followed;

(B) that, upon the request of the applicant, a specified landlord, custodian, or other specified person furnish the applicant forthwith all information, facilities, or assistance necessary to accomplish the physical search in such a manner as will protect its secrecy and produce a minimum of interference with the services that such landlord, custodian, or other person is providing the target of the physical search;

(C) that such landlord, custodian, or other person maintain under security procedures approved by the Attorney General and the Director of National Intelligence any records concerning the search or the aid furnished that such person wishes to retain;

(D) that the applicant compensate, at the prevailing rate, such landlord, custodian, or other person for furnishing such aid; and

(E) that the Federal officer conducting the physical search promptly report to the court the circumstances and results of the physical search.

(d)(1) An order issued under this section may approve a physical search for the period necessary to achieve its purpose, or for 90 days, whichever is less, except that

(A) an order under this section shall approve a physical search targeted against a foreign power, for the period specified in the application or for one year, whichever is less, and

(B) an order under this section for a physical search targeted against an agent of a foreign power who is not a United States person may be for the period specified in the application or for one year, whichever is less.

(2) At or before the end of the period of time for which a physical search is approved by an order or an extension, or at any time after a physical search is carried out, the judge may assess compliance with the minimization procedures by reviewing the circumstances under which information concerning United States persons was acquired, retained, or disseminated.

(e)(1) Notwithstanding any other provision of this title, the Attorney General may authorize the emergency employment of a physical search if the Attorney General—

(A) reasonably determines that an emergency situation exists with respect to the employment of a physical search to obtain foreign intelligence information before an order authorizing such physical search can with due diligence be obtained;

(B) reasonably determines that the factual basis for issuance of an order under this title to approve such physical search exists;

(C) informs, either personally or through a designee, a judge of the Foreign Intelligence Surveillance Court at the time of such authorization that the decision has been made to employ an emergency physical search; and

(D) makes an application in accordance with this title to a judge of the Foreign Intelligence Surveillance Court as soon as practicable, but not more than 7 days after the Attorney General authorizes such physical search.

(2) If the Attorney General authorizes the emergency employment of a physical search under paragraph (1), the Attorney General shall require that the minimization procedures required by this title for the issuance of a judicial order be followed.

(3) In the absence of a judicial order approving such physical search, the physical search shall terminate when the information sought is obtained, when the application for the order is denied, or after the expiration of 7

days from the time of authorization by the Attorney General, whichever is earliest.

(4) A denial of the application made under this subsection may be reviewed as provided in section 103.

(5) In the event that such application for approval is denied, or in any other case where the physical search is terminated and no order is issued approving the physical search, no information obtained or evidence derived from such physical search shall be received in evidence or otherwise disclosed in any trial, hearing, or other proceeding in or before any court, grand jury, department, office, agency, regulatory body, legislative committee, or other authority of the United States, a State, or political subdivision thereof, and no information concerning any United States person acquired from such physical search shall subsequently be used or disclosed in any other manner by Federal officers or employees without the consent of such person, except with the approval of the Attorney General if the information indicates a threat of death or serious bodily harm to any person.

(6) The Attorney General shall assess compliance with the requirements of paragraph (5).

(f) Applications made and orders granted under this title shall be retained for a period of at least 10 years from the date of the application.

USE OF INFORMATION

SEC. 305. [50 U.S.C. § 1825]

(a) Information acquired from a physical search conducted pursuant to this title concerning any United States person may be used and disclosed by Federal officers and employees without the consent of the United States person only in accordance with the minimization procedures required by this title. No information acquired from a physical search pursuant to this title may be used or disclosed by Federal officers or employees except for lawful purposes.

(b) Where a physical search authorized and conducted pursuant to section 304 involves the residence of a United States person, and, at any time after the search the Attorney General determines there is no national security interest in continuing to maintain the secrecy of the search, the Attorney General shall provide notice to the United States person whose residence was searched of the fact of the search conducted pursuant to this Act and shall identify any property of such person seized, altered, or reproduced during such search.

(c) No information acquired pursuant to this title shall be disclosed for law enforcement purposes unless such disclosure is accompanied by a statement that

such information, or any information derived therefrom, may only be used in a criminal proceeding with the advance authorization of the Attorney General.

(d) Whenever the United States intends to enter into evidence or otherwise use or disclose in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, against an aggrieved person, any information obtained or derived from a physical search pursuant to the authority of this Act, the United States shall, prior to the trial, hearing, or the other proceeding or at a reasonable time prior to an effort to so disclose or so use that information or submit it in evidence, notify the aggrieved person and the court or other authority in which the information is to be disclosed or used that the United States intends to so disclose or so use such information.

(e) Whenever any State or political subdivision thereof intends to enter into evidence or otherwise use or disclose in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of a State or a political subdivision thereof against an aggrieved person any information obtained or derived from a physical search pursuant to the authority of this Act, the State or political subdivision thereof shall notify the aggrieved person, the court or other authority in which the information is to be disclosed or used, and the Attorney General that the State or political subdivision thereof intends to so disclose or so use such information.

(f)(1) Any person against whom evidence obtained or derived from a physical search to which he is an aggrieved person is to be, or has been, introduced or otherwise used or disclosed in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, a State, or a political subdivision thereof, may move to suppress the evidence obtained or derived from such search on the grounds that—

(A) the information was unlawfully acquired; or

(B) the physical search was not made in conformity with an order of authorization or approval.

(2) Such a motion shall be made before the trial, hearing, or other proceeding unless there was no opportunity to make such a motion or the person was not aware of the grounds of the motion.

(g) Whenever a court or other authority is notified pursuant to subsection (d) or (e), or whenever a motion is made pursuant to subsection (f), or whenever any motion or request is made by an aggrieved person pursuant to any other statute or rule of the United States or any State before any court or other authority of the United States or any State to discover or obtain applications or orders or other materials relating to a physical search authorized by this title or to discover, obtain, or suppress evidence or information obtained or derived from a physical search authorized by this title, the United States district court or, where the

motion is made before another authority, the United States district court in the same district as the authority shall, notwithstanding any other provision of law, if the Attorney General files an affidavit under oath that disclosure or any adversary hearing would harm the national security of the United States, review in camera and ex parte the application, order, and such other materials relating to the physical search as may be necessary to determine whether the physical search of the aggrieved person was lawfully authorized and conducted. In making this determination, the court may disclose to the aggrieved person, under appropriate security procedures and protective orders, portions of the application, order, or other materials relating to the physical search, or may require the Attorney General to provide to the aggrieved person a summary of such materials, only where such disclosure is necessary to make an accurate determination of the legality of the physical search.

(h) If the United States district court pursuant to subsection (g) determines that the physical search was not lawfully authorized or conducted, it shall, in accordance with the requirements of law, suppress the evidence which was unlawfully obtained or derived from the physical search of the aggrieved person or otherwise grant the motion of the aggrieved person. If the court determines that the physical search was lawfully authorized or conducted, it shall deny the motion of the aggrieved person except to the extent that due process requires discovery or disclosure.

(i) Orders granting motions or requests under subsection (h), decisions under this section that a physical search was not lawfully authorized or conducted, and orders of the United States district court requiring review or granting disclosure of applications, orders, or other materials relating to the physical search shall be final orders and binding upon all courts of the United States and the several States except a United States Court of Appeals or the Supreme Court.

(j)(1) If an emergency execution of a physical search is authorized under section 304(d) and a subsequent order approving the search is not obtained, the judge shall cause to be served on any United States person named in the application and on such other United States persons subject to the search as the judge may determine in his discretion it is in the interests of justice to serve, notice of—

- (A) the fact of the application;
- (B) the period of the search; and
- (C) the fact that during the period information was or was not obtained.

(2) On an ex parte showing of good cause to the judge, the serving of the notice required by this subsection may be postponed or suspended for a period not to exceed 90 days. Thereafter, on a further ex parte showing of good cause, the court shall forego ordering the serving of the notice required under this subsection.

(k)(1) Federal officers who conduct physical searches to acquire foreign intelligence information under this title may consult with Federal law enforcement officers or law enforcement personnel of a State or political subdivision of a State (including the chief executive officer of that State or political subdivision who has the authority to appoint or direct the chief law enforcement officer of that State or political subdivision) to coordinate efforts to investigate or protect against—

(A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;

(B) sabotage, international terrorism, or the international proliferation of weapons of mass destruction by a foreign power or an agent of a foreign power; or

(C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power.

(2) Coordination authorized under paragraph (1) shall not preclude the certification required by section 303(a)(6) or the entry of an order under section 304.

CONGRESSIONAL OVERSIGHT

SEC. 306. [50 U.S.C. § 1826]

On a semiannual basis the Attorney General shall fully inform the Permanent Select Committee on Intelligence and the Committee on the Judiciary of the House of Representatives and the Select Committee on Intelligence and the Committee on the Judiciary of the Senate concerning all physical searches conducted pursuant to this title. On a semiannual basis the Attorney General shall also provide to those committees a report setting forth with respect to the preceding six-month period—

(1) the total number of applications made for orders approving physical searches under this title;

(2) the total number of such orders either granted, modified, or denied;

(3) the number of physical searches which involved searches of the residences, offices, or personal property of United States persons, and the number of occasions, if any, where the Attorney General provided notice pursuant to section 305(b); and

(4) the total number of emergency physical searches authorized by the Attorney General under section 304(e) and the total number of subsequent orders approving or denying such physical searches.

PENALTIES

SEC. 307. [50 U.S.C. § 1827]

(a) A person is guilty of an offense if he intentionally—

(1) under color of law for the purpose of obtaining foreign intelligence information, executes a physical search within the United States except as authorized by statute; or

(2) discloses or uses information obtained under color of law by physical search within the United States, knowing or having reason to know that the information was obtained through physical search not authorized by statute, for the purpose of obtaining intelligence information.

(b) It is a defense to a prosecution under subsection (a) that the defendant was a law enforcement or investigative officer engaged in the course of his official duties and the physical search was authorized by and conducted pursuant to a search warrant or court order of a court of competent jurisdiction.

(c) An offense described in this section is punishable by a fine of not more than \$10,000 or imprisonment for not more than five years, or both.

(d) There is Federal jurisdiction over an offense under this section if the person committing the offense was an officer or employee of the United States at the time the offense was committed.

CIVIL LIABILITY

SEC. 308. [50 U.S.C. § 1828]

An aggrieved person, other than a foreign power or an agent of a foreign power, as defined in section 101 (a) or (b)(1)(A), respectively, of this Act, whose premises, property, information, or material has been subjected to a physical search within the United States or about whom information obtained by such a physical search has been disclosed or used in violation of section 307 shall have a cause of action against any person who committed such violation and shall be entitled to recover—

(1) actual damages, but not less than liquidated damages of \$1,000 or \$100 per day for each day of violation, whichever is greater;

(2) punitive damages; and

(3) reasonable attorney's fees and other investigative and litigation costs reasonably incurred.

AUTHORIZATION DURING TIME OF WAR

SEC. 309. [50 U.S.C. § 1829]

Notwithstanding any other provision of law, the President, through the Attorney General, may authorize physical searches without a court order under this title to acquire foreign intelligence information for a period not to exceed 15 calendar days following a declaration of war by the Congress.

**TITLE IV—PEN REGISTERS AND TRAP AND TRACE DEVICES
FOR FOREIGN INTELLIGENCE PURPOSES**

DEFINITIONS

SEC. 401. [50 U.S.C. § 1841]

As used in this title:

- (1) The terms “foreign power”, “agent of a foreign power”, “international terrorism”, “foreign intelligence information”, “Attorney General”, “United States person”, “United States”, “person”, and “State” shall have the same meanings as in section 101 of this Act.
- (2) The terms “pen register” and “trap and trace device” have the meanings given such terms in section 3127 of title 18, United States Code.
- (3) The term “aggrieved person” means any person—
 - (A) whose telephone line was subject to the installation or use of a pen register or trap and trace device authorized by this title; or
 - (B) whose communication instrument or device was subject to the use of a pen register or trap and trace device authorized by this title to capture incoming electronic or other communications impulses.
- (4)(A) The term “specific selection term”—
 - (i) is a term that specifically identifies a person, account, address, or personal device, or any other specific identifier; and
 - (ii) is used to limit, to the greatest extent reasonably practicable, the scope of information sought, consistent with the purpose for seeking the use of the pen register or trap and trace device.
- (B) A specific selection term under subparagraph (A) does not include an identifier that does not limit, to the greatest extent reasonably practicable, the scope of information sought, consistent with the purpose for seeking the use of the pen register or trap and trace device, such as an identifier that—
 - (i) identifies an electronic communication service provider (as that term is defined in section 701) or a provider of remote computing service (as that term is defined in section 2711 of title

18, United States Code), when not used as part of a specific identifier as described in subparagraph (A), unless the provider is itself a subject of an authorized investigation for which the specific selection term is used as the basis for the use; or (ii) identifies a broad geographic region, including the United States, a city, a county, a State, a zip code, or an area code, when not used as part of a specific identifier as described in subparagraph (A).

(C) For purposes of subparagraph (A), the term “address” means a physical address or electronic address, such as an electronic mail address or temporarily assigned network address (including an Internet protocol address).

(D) Nothing in this paragraph shall be construed to preclude the use of multiple terms or identifiers to meet the requirements of subparagraph (A).

PEN REGISTERS AND TRAP AND TRACE DEVICES FOR FOREIGN INTELLIGENCE AND INTERNATIONAL TERRORISM INVESTIGATIONS

SEC. 402. [50 U.S.C. § 1842]

(a)(1) Notwithstanding any other provision of law, the Attorney General or a designated attorney for the Government may make an application for an order or an extension of an order authorizing or approving the installation and use of a pen register or trap and trace device for any investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution which is being conducted by the Federal Bureau of Investigation under such guidelines as the Attorney General approves pursuant to Executive Order No. 12333, or a successor order.

(2) The authority under paragraph (1) is in addition to the authority under title I of this Act to conduct the electronic surveillance referred to in that paragraph.

(b) Each application under this section shall be in writing under oath or affirmation to—

(1) a judge of the court established by section 103(a) of this Act; or

(2) a United States Magistrate Judge under chapter 43 of title 28, United States Code, who is publicly designated by the Chief Justice of the United States to have the power to hear applications for and grant orders

approving the installation and use of a pen register or trap and trace device on behalf of a judge of that court.

(c) Each application under this section shall require the approval of the Attorney General, or a designated attorney for the Government, and shall include—

(1) the identity of the Federal officer seeking to use the pen register or trap and trace device covered by the application;

(2) a certification by the applicant that the information likely to be obtained is foreign intelligence information not concerning a United States person or is relevant to an ongoing investigation to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution;

(3) a specific selection term to be used as the basis for the use of the pen register or trap and trace device;

(4) a certification by the Federal Officer seeking to use the pen register or trap and trace device covered by the application that, to the best knowledge of the Federal Officer, the Attorney General or a designated attorney for the Government has been apprised of all information that might reasonably—

(A) call into question the accuracy of the application or the reasonableness of any assessment in the application conducted by the department or agency on whose behalf the application is made; or

(B) otherwise raise doubts with respect to the findings required under subsection (d); and

(5) non-cumulative information known to the Federal officer seeking to use the pen register or trap and trace device covered by the application, that is potentially exculpatory regarding the requested legal findings or any assessment in the application.

(d)(1) Upon an application made pursuant to this section, the judge shall enter an ex parte order as requested, or as modified, approving the installation and use of a pen register or trap and trace device if the judge finds that the application satisfies the requirements of this section.

(2) An order issued under this section—

(A) shall specify—

(i) the identity, if known, of the person who is the subject of the investigation;

(ii) the identity, if known, of the person to whom is leased or in whose name is listed the telephone line or

other facility to which the pen register or trap and trace device is to be attached or applied; and
(iii) the attributes of the communications to which the order applies, such as the number or other identifier, and, if known, the location of the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied and, in the case of a trap and trace device, the geographic limits of the trap and trace order;

(B) shall direct that—

(i) upon request of the applicant, the provider of a wire or electronic communication service, landlord, custodian, or other person shall furnish any information, facilities, or technical assistance necessary to accomplish the installation and operation of the pen register or trap and trace device in such a manner as will protect its secrecy and produce a minimum amount of interference with the services that such provider, landlord, custodian, or other person is providing the person concerned;

(ii) such provider, landlord, custodian, or other person—

(I) shall not disclose the existence of the investigation or of the pen register or trap and trace device to any person unless or until ordered by the court; and

(II) shall maintain, under security procedures approved by the Attorney General and the Director of National Intelligence pursuant to section 105(b)(2)(C) of this Act, any records concerning the pen register or trap and trace device or the aid furnished; and

(iii) the applicant shall compensate such provider, landlord, custodian, or other person for reasonable expenses incurred by such provider, landlord, custodian, or other person in providing such information, facilities, or technical assistance; and

(C) shall direct that, upon the request of the applicant, the provider of a wire or electronic communication service shall disclose to the Federal officer using the pen register or trap and trace device covered by the order—

(i) in the case of the customer or subscriber using the service covered by the order (for the period specified by the order)—

- (I) the name of the customer or subscriber;
- (II) the address of the customer or subscriber;
- (III) the telephone or instrument number, or other subscriber number or identifier, of the customer or subscriber, including any temporarily assigned network address or associated routing or transmission information;
- (IV) the length of the provision of service by such provider to the customer or subscriber and the types of services utilized by the customer or subscriber;
- (V) in the case of a provider of local or long distance telephone service, any local or long distance telephone records of the customer or subscriber;
- (VI) if applicable, any records reflecting period of usage (or sessions) by the customer or subscriber; and
- (VII) any mechanisms and sources of payment for such service, including the number of any credit card or bank account utilized for payment for such service; and

(ii) if available, with respect to any customer or subscriber of incoming or outgoing communications to or from the service covered by the order—

- (I) the name of such customer or subscriber;
- (II) the address of such customer or subscriber;
- (III) the telephone or instrument number, or other subscriber number or identifier, of such customer or subscriber, including any temporarily assigned network address or associated routing or transmission information; and
- (IV) the length of the provision of service by such provider to such customer or subscriber and the types of services utilized by such customer or subscriber.

(3) A denial of the application made under this subsection may be reviewed as provided in section 103.

(e)(1) Except as provided in paragraph (2), an order issued under this section shall authorize the installation and use of a pen register or trap and trace device for a period not to exceed 90 days. Extensions of such an order may be granted, but only upon an application for an order under this section and upon the judicial finding required by subsection (d). The period of extension shall be for a period not to exceed 90 days.

(2) In the case of an application under subsection (c) where the applicant has certified that the information likely to be obtained is foreign intelligence information not concerning a United States person, an order, or an extension of an order, under this section may be for a period not to exceed one year.

(f) No cause of action shall lie in any court against any provider of a wire or electronic communication service, landlord, custodian, or other person (including any officer, employee, agent, or other specified person thereof) that furnishes any information, facilities, or technical assistance under subsection (d) in accordance with the terms of an order issued under this section.

(g) Unless otherwise ordered by the judge, the results of a pen register or trap and trace device shall be furnished at reasonable intervals during regular business hours for the duration of the order to the authorized Government official or officials.

(h) **PRIVACY PROCEDURES.**—

(1) **IN GENERAL.**—The Attorney General shall ensure that appropriate policies and procedures are in place to safeguard nonpublicly available information concerning United States persons that is collected through the use of a pen register or trap and trace device installed under this section. Such policies and procedures shall, to the maximum extent practicable and consistent with the need to protect national security, include privacy protections that apply to the collection, retention, and use of information concerning United States persons.

(2) **RULE OF CONSTRUCTION.**—Nothing in this subsection limits the authority of the court established under section 103(a) or of the Attorney General to impose additional privacy or minimization procedures with regard to the installation or use of a pen register or trap and trace device.

AUTHORIZATION DURING EMERGENCIES

SEC. 403. [50 U.S.C. § 1843]

(a) Notwithstanding any other provision of this title, when the Attorney General makes a determination described in subsection (b), the Attorney General may

authorize the installation and use of a pen register or trap and trace device on an emergency basis to gather foreign intelligence information not concerning a United States person or information to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution if—

- (1) a judge referred to in section 402(b) of this Act is informed by the Attorney General or his designee at the time of such authorization that the decision has been made to install and use the pen register or trap and trace device, as the case may be, on an emergency basis; and
- (2) an application in accordance with section 402 of this Act is made to such judge as soon as practicable, but not more than 7 days, after the Attorney General authorizes the installation and use of the pen register or trap and trace device, as the case may be, under this section.

(b) A determination under this subsection is a reasonable determination by the Attorney General that—

- (1) an emergency requires the installation and use of a pen register or trap and trace device to obtain foreign intelligence information not concerning a United States person or information to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution before an order authorizing the installation and use of the pen register or trap and trace device, as the case may be, can with due diligence be obtained under section 402 of this Act; and
- (2) the factual basis for issuance of an order under such section 402 to approve the installation and use of the pen register or trap and trace device, as the case may be, exists.

(c)(1) In the absence of an order applied for under subsection (a)(2) approving the installation and use of a pen register or trap and trace device authorized under this section, the installation and use of the pen register or trap and trace device, as the case may be, shall terminate at the earlier of—

- (A) when the information sought is obtained;
- (B) when the application for the order is denied under section 402 of this Act; or
- (C) 7 days after the time of the authorization by the Attorney General.

(2) In the event that an application for an order applied for under subsection (a)(2) is denied, or in any other case where the installation and use of a pen register or trap and trace device under this section is terminated and no order under section 402 of this Act is issued approving

the installation and use of the pen register or trap and trace device, as the case may be, no information obtained or evidence derived from the use of the pen register or trap and trace device, as the case may be, shall be received in evidence or otherwise disclosed in any trial, hearing, or other proceeding in or before any court, grand jury, department, office, agency, regulatory body, legislative committee, or other authority of the United States, a State, or political subdivision thereof, and no information concerning any United States person acquired from the use of the pen register or trap and trace device, as the case may be, shall subsequently be used or disclosed in any other manner by Federal officers or employees without the consent of such person, except with the approval of the Attorney General if the information indicates a threat of death or serious bodily harm to any person.

(3) A denial of the application made under subsection (a)(2) may be reviewed as provided in section 103.

(d) PRIVACY PROCEDURES.—Information collected through the use of a pen register or trap and trace device installed under this section shall be subject to the policies and procedures required under section 402(h).

AUTHORIZATION DURING TIME OF WAR

SEC. 404. [50 U.S.C. § 1844]

Notwithstanding any other provision of law, the President, through the Attorney General, may authorize the use of a pen register or trap and trace device without a court order under this title to acquire foreign intelligence information for a period not to exceed 15 calendar days following a declaration of war by Congress.

USE OF INFORMATION

SEC. 405. [50 U.S.C. § 1845]

(a)(1) Information acquired from the use of a pen register or trap and trace device installed pursuant to this title concerning any United States person may be used and disclosed by Federal officers and employees without the consent of the United States person only in accordance with the provisions of this section.

(2) No information acquired from a pen register or trap and trace device installed and used pursuant to this title may be used or disclosed by Federal officers or employees except for lawful purposes.

(b) No information acquired pursuant to this title shall be disclosed for law enforcement purposes unless such disclosure is accompanied by a statement that

such information, or any information derived therefrom, may only be used in a criminal proceeding with the advance authorization of the Attorney General.

(c) Whenever the United States intends to enter into evidence or otherwise use or disclose in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States against an aggrieved person any information obtained or derived from the use of a pen register or trap and trace device pursuant to this title, the United States shall, before the trial, hearing, or the other proceeding or at a reasonable time before an effort to so disclose or so use that information or submit it in evidence, notify the aggrieved person and the court or other authority in which the information is to be disclosed or used that the United States intends to so disclose or so use such information.

(d) Whenever any State or political subdivision thereof intends to enter into evidence or otherwise use or disclose in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the State or political subdivision thereof against an aggrieved person any information obtained or derived from the use of a pen register or trap and trace device pursuant to this title, the State or political subdivision thereof shall notify the aggrieved person, the court or other authority in which the information is to be disclosed or used, and the Attorney General that the State or political subdivision thereof intends to so disclose or so use such information.

(e)(1) Any aggrieved person against whom evidence obtained or derived from the use of a pen register or trap and trace device is to be, or has been, introduced or otherwise used or disclosed in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, or a State or political subdivision thereof, may move to suppress the evidence obtained or derived from the use of the pen register or trap and trace device, as the case may be, on the grounds that—

(A) the information was unlawfully acquired; or

(B) the use of the pen register or trap and trace device, as the case may be, was not made in conformity with an order of authorization or approval under this title.

(2) A motion under paragraph (1) shall be made before the trial, hearing, or other proceeding unless there was no opportunity to make such a motion or the aggrieved person concerned was not aware of the grounds of the motion.

(f)(1) Whenever a court or other authority is notified pursuant to subsection (c) or (d), whenever a motion is made pursuant to subsection (e), or whenever any motion or request is made by an aggrieved person pursuant to any other statute or rule of the United States or any State before any court or other authority of the United States or any State to discover or obtain applications or orders or other

materials relating to the use of a pen register or trap and trace device authorized by this title or to discover, obtain, or suppress evidence or information obtained or derived from the use of a pen register or trap and trace device authorized by this title, the United States district court or, where the motion is made before another authority, the United States district court in the same district as the authority shall, notwithstanding any other provision of law and if the Attorney General files an affidavit under oath that disclosure or any adversary hearing would harm the national security of the United States, review in camera and ex parte the application, order, and such other materials relating to the use of the pen register or trap and trace device, as the case may be, as may be necessary to determine whether the use of the pen register or trap and trace device, as the case may be, was lawfully authorized and conducted.

(2) In making a determination under paragraph (1), the court may disclose to the aggrieved person, under appropriate security procedures and protective orders, portions of the application, order, or other materials relating to the use of the pen register or trap and trace device, as the case may be, or may require the Attorney General to provide to the aggrieved person a summary of such materials, only where such disclosure is necessary to make an accurate determination of the legality of the use of the pen register or trap and trace device, as the case may be.

(g)(1) If the United States district court determines pursuant to subsection (f) that the use of a pen register or trap and trace device was not lawfully authorized or conducted, the court may, in accordance with the requirements of law, suppress the evidence which was unlawfully obtained or derived from the use of the pen register or trap and trace device, as the case may be, or otherwise grant the motion of the aggrieved person.

(2) If the court determines that the use of the pen register or trap and trace device, as the case may be, was lawfully authorized or conducted, it may deny the motion of the aggrieved person except to the extent that due process requires discovery or disclosure.

(h) Orders granting motions or requests under subsection (g), decisions under this section that the use of a pen register or trap and trace device was not lawfully authorized or conducted, and orders of the United States district court requiring review or granting disclosure of applications, orders, or other materials relating to the installation and use of a pen register or trap and trace device shall be final orders and binding upon all courts of the United States and the several States except a United States Court of Appeals or the Supreme Court.

CONGRESSIONAL OVERSIGHT

SEC. 406. [50 U.S.C. § 1846]

(a) On a semiannual basis, the Attorney General shall fully inform the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate, and the Committee on the Judiciary of the House of Representatives and the Committee on the Judiciary of the Senate, concerning all uses of pen registers and trap and trace devices pursuant to this title.

(b) On a semiannual basis, the Attorney General shall also provide to the committees referred to in subsection (a) a report setting forth with respect to the preceding 6-month period—

(1) the total number of applications made for orders approving the use of pen registers or trap and trace devices under this title;

(2) the total number of such orders either granted, modified, or denied;

(3) the total number of pen registers and trap and trace devices whose installation and use was authorized by the Attorney General on an emergency basis under section 403, and the total number of subsequent orders approving or denying the installation and use of such pen registers and trap and trace devices;

(4) each department or agency on behalf of which the Attorney General or a designated attorney for the Government has made an application for an order authorizing or approving the installation and use of a pen register or trap and trace device under this title;

(5) for each department or agency described in paragraph (4), each number described in paragraphs (1), (2), and (3); and

(6) a good faith estimate of the total number of subjects who were targeted by the installation and use of a pen register or trap and trace device under an order or emergency authorization issued under this title, rounded to the nearest 500, including—

(A) the number of such subjects who are United States persons, reported to the nearest band of 500, starting with 0-499; and

(B) of the number of United States persons described in subparagraph (A), the number of persons whose information acquired pursuant to such order was reviewed or accessed by a Federal officer, employee, or agent, reported to the nearest band of 500, starting with 0-499.

(c) Each report under subsection (b) shall be submitted in unclassified form, to the extent consistent with national security. Not later than 7 days after the date on which the Attorney General submits such a report, the Attorney General shall make the report publicly available, or, if the Attorney General determines that the

report cannot be made publicly available consistent with national security, the Attorney General may make publicly available an unclassified summary of the report or a redacted version of the report.

**TITLE V—ACCESS TO CERTAIN BUSINESS RECORDS
FOR FOREIGN INTELLIGENCE PURPOSES**

DEFINITIONS

SEC. 501. [50 U.S.C. § 1861]

As used in this title:

(1) The terms “foreign power”, “agent of a foreign power”, “foreign intelligence information”, “international terrorism”, and “Attorney General” shall have the same meanings as in section 101 of this Act.

(2) The term “common carrier” means any person or entity transporting people or property by land, rail, water, or air for compensation.

(3) The term “physical storage facility” means any business or entity that provides space for the storage of goods or materials, or services related to the storage of goods or materials, to the public or any segment thereof.

(4) The term “public accommodation facility” means any inn, hotel, motel, or other establishment that provides lodging to transient guests.

(5) The term “vehicle rental facility” means any person or entity that provides vehicles for rent, lease, loan, or other similar use to the public or any segment thereof.

**ACCESS TO CERTAIN BUSINESS RECORDS FOR FOREIGN INTELLIGENCE
AND INTERNATIONAL TERRORISM INVESTIGATIONS**

SEC. 502. [50 U.S.C. § 1862]

(a) The Director of the Federal Bureau of Investigation or a designee of the Director (whose rank shall be no lower than Assistant Special Agent in Charge) may make an application for an order authorizing a common carrier, public accommodation facility, physical storage facility, or vehicle rental facility to release records in its possession for an investigation to gather foreign intelligence information or an investigation concerning international terrorism which investigation is being conducted by the Federal Bureau of Investigation under such guidelines as the Attorney General approves pursuant to Executive Order No. 12333, or a successor order.

(b) Each application under this section—

(1) shall be made to—

(A) a judge of the court established by section 103(a) of this Act; or

(B) a United States Magistrate Judge under chapter 43 of title 28, United States Code, who is publicly designated by the Chief Justice of the United States to have the power to hear applications and grant orders for release of records under this section on behalf of a judge of that court; and

(2) shall specify that—

(A) the records concerned are sought for an investigation described in subsection (a);

(B) there are specific and articulable facts giving reason to believe that the person to whom the records pertain is a foreign power or an agent of a foreign power;

(E)³ a statement by the applicant that, to the best knowledge of the applicant, the application fairly reflects all information that might reasonably—

(i) call into question the accuracy of the application or the reasonableness of any assessment in the application conducted by the department or agency on whose behalf the application is made; or

(ii) otherwise raise doubts with respect to the findings required under subsection (c); and

(F) non-cumulative information known to the applicant that is potentially exculpatory regarding the requested legal findings or any assessment in the application.

(c)(1) Upon an application made pursuant to this section, the judge shall enter an ex parte order as requested, or as modified, approving the release of records if the judge finds that the application meets the requirements of this section..

(2) An order under this subsection shall not disclose that it is issued for purposes of an investigation described in subsection (a).

(d)(1) Any common carrier, public accommodation facility, physical storage facility, or vehicle rental facility shall comply with an order under subsection (c).

(2) No common carrier, public accommodation facility, physical storage facility, or vehicle rental facility, or officer, employee, or agent thereof shall disclose to any other person (other than those officers, agents, or employees of such common carrier, public accommodation facility, physical storage facility, or vehicle rental facility necessary to fulfill the requirement to disclose information to the Federal Bureau of Investigation under this section) that the Federal Bureau

³ So in original. No subpars. (C) and (D) have been enacted.

of Investigation has sought or obtained records pursuant to an order under this section.

CONGRESSIONAL OVERSIGHT

SEC. 503. [50 U.S.C. § 1863]

(a) On an semiannual basis, the Attorney General shall fully inform the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate concerning all requests for records under this title.

(b) On an semiannual basis, the Attorney General shall provide to the Committees on the Judiciary of the House of Representatives and the Senate a report setting forth with respect to the preceding 6-month period—

- (1) the total number of applications made for orders approving requests for records under this title; and
- (3) the total number of such orders either granted, modified, or denied.

TITLE VI—OVERSIGHT

SEMIANNUAL REPORT OF THE ATTORNEY GENERAL

SEC. 601. [50 U.S.C. § 1871]

(a) REPORT.—On a semiannual basis, the Attorney General shall submit to the Permanent Select Committee on Intelligence of the House of Representatives, the Select Committee on Intelligence of the Senate, and the Committees on the Judiciary of the House of Representatives and the Senate, in a manner consistent with the protection of the national security, a report setting forth with respect to the preceding 6-month period—

- (1) the aggregate number of persons targeted for orders issued under this Act, including a breakdown of those targeted for—
 - (A) electronic surveillance under section 105;
 - (B) physical searches under section 304;
 - (C) pen registers under section 402;
 - (D) access to records under section 501;
 - (E) acquisitions under section 703; and
 - (F) acquisitions under section 704;
- (2) the number of individuals covered by an order issued pursuant to section 101(b)(1)(C);
- (3) the number of times that the Attorney General has authorized that information obtained under this Act may be used in a criminal

proceeding or any information derived therefrom may be used in a criminal proceeding;

(4) a summary of significant legal interpretations of this Act involving matters before the Foreign Intelligence Surveillance Court or the Foreign Intelligence Surveillance Court of Review, including interpretations presented in applications or pleadings filed with the Foreign Intelligence Surveillance Court or the Foreign Intelligence Surveillance Court of Review by the Department of Justice; and

(5) copies of all decisions, orders, or opinions of the Foreign Intelligence Surveillance Court or Foreign Intelligence Surveillance Court of Review that include significant construction or interpretation of the provisions of this Act.

(b) FREQUENCY.—The first report under this section shall be submitted not later than 6 months after the date of enactment of this section. Subsequent reports under this section shall be submitted semi-annually thereafter.

(c) SUBMISSIONS TO CONGRESS.—The Attorney General shall submit to the committees of Congress referred to in subsection (a)—

(1) not later than 45 days after the date on which the Foreign Intelligence Surveillance Court or the Foreign Intelligence Surveillance Court of Review issues a decision, order, or opinion, including any denial or modification of an application under this Act, that includes significant construction or interpretation of any provision of law or results in a change of application of any provision of this Act or a novel application of any provision of this Act, a copy of such decision, order, or opinion and any pleadings, applications, or memoranda of law associated with such decision, order, or opinion;

(2) a copy of each such decision, order, or opinion, and any pleadings, applications, or memoranda of law associated with such decision, order, or opinion, that was issued during the 5-year period ending on the date of the enactment of the FISA Amendments Act of 2008 and not previously submitted in a report under subsection (a);

(3) for any hearing, oral argument, or other proceeding before the Foreign Intelligence Surveillance Court or Foreign Intelligence Surveillance Court of Review for which a court reporter produces a transcript, not later than 45 days after the government receives the final transcript or the date on which the matter of the hearing, oral argument, or other proceeding is resolved, whichever is later, a notice of the existence of such transcript. Not later than three business days after a committee referred to in subsection (a) requests to review an existing transcript, the Attorney General shall facilitate such request; and

(4) a copy of each declassified document that has undergone review under section 602.

(d) PROTECTION OF NATIONAL SECURITY.—The Attorney General, in consultation with the Director of National Intelligence, may authorize redactions of materials described in subsection (c) that are provided to the committees of Congress referred to in subsection (a), if such redactions are necessary to protect the national security of the United States and are limited to sensitive sources and methods information or the identities of targets.

(e) DEFINITIONS.—In this section:

(1) FOREIGN INTELLIGENCE SURVEILLANCE COURT.—The term “Foreign Intelligence Surveillance Court” means the court established under section 103(a).

(2) FOREIGN INTELLIGENCE SURVEILLANCE COURT OF REVIEW.—The term “Foreign Intelligence Surveillance Court of Review” means the court established under section 103(b).

DECLASSIFICATION OF SIGNIFICANT DECISIONS, ORDERS, AND OPINIONS

SEC. 602. [50 U.S.C. § 1872]

(a) DECLASSIFICATION REQUIRED.—Subject to subsection (b), the Director of National Intelligence, in consultation with the Attorney General, shall conduct a declassification review, to be concluded as soon as practicable, but not later than 180 days after the commencement of such review, of each decision, order, or opinion issued by the Foreign Intelligence Surveillance Court or the Foreign Intelligence Surveillance Court of Review (as defined in section 601(e)) that includes a significant construction or interpretation of any provision of law, including any novel or significant construction or interpretation of the term “specific selection term”, and, consistent with that review, make publicly available to the greatest extent practicable each such decision, order, or opinion.

(b) REDACTED FORM.—The Director of National Intelligence, in consultation with the Attorney General, may satisfy the requirement under subsection (a) to make a decision, order, or opinion described in such subsection publicly available to the greatest extent practicable by making such decision, order, or opinion publicly available in redacted form.

(c) NATIONAL SECURITY WAIVER.—The Director of National Intelligence, in consultation with the Attorney General, may waive the requirement to declassify and make publicly available a particular decision, order, or opinion under subsection (a), if—

(1) the Director of National Intelligence, in consultation with the Attorney General, determines that a waiver of such requirement is

necessary to protect the national security of the United States or properly classified intelligence sources or methods; and

(2) the Director of National Intelligence makes publicly available an unclassified statement prepared by the Attorney General, in consultation with the Director of National Intelligence—

(A) summarizing the significant construction or interpretation of any provision of law, which shall include, to the extent consistent with national security, a description of the context in which the matter arises and any significant construction or interpretation of any statute, constitutional provision, or other legal authority relied on by the decision; and

(B) that specifies that the statement has been prepared by the Attorney General and constitutes no part of the opinion of the Foreign Intelligence Surveillance Court or the Foreign Intelligence Surveillance Court of Review.

ANNUAL REPORTS

SEC. 603. [50 U.S.C. § 1873]

(a) REPORT BY DIRECTOR OF THE ADMINISTRATIVE OFFICE OF THE UNITED STATES COURTS.—

(1) REPORT REQUIRED.—The Director of the Administrative Office of the United States Courts shall annually submit to the Permanent Select Committee on Intelligence and the Committee on the Judiciary of the House of Representatives and the Select Committee on Intelligence and the Committee on the Judiciary of the Senate, subject to a declassification review by the Attorney General and the Director of National Intelligence, a report that includes—

(A) the number of applications or certifications for orders submitted under each of sections 105, 304, 402, 501, 702, 703, and 704;

(B) the number of such orders granted under each of those sections;

(C) the number of orders modified under each of those sections;

(D) the number of applications or certifications denied under each of those sections;

(E) the number of appointments of an individual to serve as amicus curiae under section 103, including the name of each individual appointed to serve as amicus curiae;

(F) the number of findings issued under section 103(i) that such appointment is not appropriate and the text of any such findings; and

(G) the number of times the Foreign Intelligence Surveillance Court and the Foreign Intelligence Surveillance Court of Review exercised authority under chapter 21 of title 18, United States Code and a description of each use of such authority.

(2) PUBLICATION.—The Director shall make the report required under paragraph (1) publicly available on an Internet Web site, except that the Director shall not make publicly available on an Internet Web site the findings described in subparagraph (F) of paragraph (1).

(b) MANDATORY REPORTING BY DIRECTOR OF NATIONAL INTELLIGENCE.—Except as provided in subsection (d), the Director of National Intelligence shall annually make publicly available on an Internet Web site a report that identifies, for the preceding 12-month period—

(1) the total number of orders issued pursuant to titles I and III and sections 703 and 704 and a good faith estimate of—

(A) the number of targets of such orders;

(B) the number of targets of such orders who are known to not be United States persons; and

(C) the number of targets of such orders who are known to be United States persons;

(2) the total number of orders issued pursuant to section 702, including pursuant to subsection (f)(2) of such section, and a good faith estimate of—

(A) the number of targets of such orders;

(B) the number of search terms concerning a known United States person used to retrieve the unminimized contents (or combined unminimized contents and noncontents information) of electronic communications or wire communications obtained through acquisitions authorized under such section, excluding the number of search terms used to prevent the return of information concerning a United States person;

(C) the number of queries concerning a known United States person of unminimized noncontents information relating to electronic communications or wire communications obtained through acquisitions authorized under such section, excluding the number of queries containing information used to prevent the return of information concerning a United States person;

(D) the number of instances in which the Federal Bureau of Investigation opened, under the Criminal Investigative Division

- or any successor division, an investigation of a United States person (who is not considered a threat to national security) based wholly or in part on an acquisition authorized under such section;
- (3) the total number of orders issued pursuant to title IV and a good faith estimate of—
- (A) the number of targets of such orders, including—
 - (i) the number of targets of such orders who are known to not be United States persons; and
 - (ii) the number of targets of such orders who are known to be United States persons; and
 - (B) the number of unique identifiers used to communicate information collected pursuant to such orders;
- (4) the number of criminal proceedings in which the United States or a State or political subdivision thereof provided notice pursuant to subsection (c) or (d) of section 106 (including with respect to information acquired from an acquisition conducted under section 702) or subsection (d) or (e) of section 305 of the intent of the government to enter into evidence or otherwise use or disclose any information obtained or derived from electronic surveillance, physical search, or an acquisition conducted pursuant to this Act;
- (5) the total number of orders issued pursuant to applications made under section 501(b)(2)(B) and a good faith estimate of—
- (A) the number of targets of such orders; and
 - (B) the number of unique identifiers used to communicate information collected pursuant to such orders;
- (6) the total number of orders issued pursuant to applications made under section 501(b)(2)(C) and a good faith estimate of—
- (A) the number of targets of such orders;
 - (B) the number of unique identifiers used to communicate information collected pursuant to such orders; and
 - (C) the number of search terms that included information concerning a United States person that were used to query any database of call detail records obtained through the use of such orders; and
- (7) the total number of national security letters issued and the number of requests for information contained within such national security letters.
- (c) TIMING.—The annual reports required by subsections (a) and (b) shall be made publicly available during April of each year and include information relating to the previous calendar year.

(d) EXCEPTIONS.—

(1) STATEMENT OF NUMERICAL RANGE.—If a good faith estimate required to be reported under subparagraph (B) of any of paragraphs (3), (5), or (6) of subsection (b) is fewer than 500, it shall be expressed as a numerical range of “fewer than 500” and shall not be expressed as an individual number.

(2) NONAPPLICABILITY TO CERTAIN INFORMATION. Paragraph (3)(B) of subsection (b) shall not apply to orders resulting in the acquisition of information by the Federal Bureau of Investigation that does not include electronic mail addresses or telephone numbers.

(3) CERTIFICATION.—

(A) IN GENERAL.—If the Director of National Intelligence concludes that a good faith estimate required to be reported under subsection (b)(2)(C) cannot be determined accurately because some but not all of the relevant elements of the intelligence community are able to provide such good faith estimate, the Director shall—

- (i) certify that conclusion in writing to the Select Committee on Intelligence and the Committee on the Judiciary of the Senate and the Permanent Select Committee on Intelligence and the Committee on the Judiciary of the House of Representatives;
- (ii) report the good faith estimate for those relevant elements able to provide such good faith estimate;
- (iii) explain when it is reasonably anticipated that such an estimate will be able to be determined fully and accurately; and
- (iv) make such certification publicly available on an Internet Web site.

(B) FORM.—A certification described in subparagraph (A) shall be prepared in unclassified form, but may contain a classified annex.

(C) TIMING.—If the Director of National Intelligence continues to conclude that the good faith estimates described in this paragraph cannot be determined accurately, the Director shall annually submit a certification in accordance with this paragraph.

(e) MANDATORY REPORTING BY DIRECTOR OF FEDERAL BUREAU OF INVESTIGATION.—The Director of the Federal Bureau of Investigation shall annually submit to the Permanent Select Committee on Intelligence and the Committee on Judiciary of the House of Representatives and the Select

Committee on Intelligence and the Committee on the Judiciary of the Senate, a report describing the accountability actions taken by the Federal Bureau of Investigation in the preceding 12-month period for noncompliant querying of information acquired under section 702 and any such actions taken pursuant to section 103(m), to include the number of ongoing personnel investigations, the outcome of any completed personnel investigations and any related adverse personnel actions taken.

(f) MANDATORY REPORTING ON SECTION 702 BY DIRECTOR OF FEDERAL BUREAU OF INVESTIGATION.—

(1) ANNUAL REPORT.—The Director of the Federal Bureau of Investigation shall annually submit to the Permanent Select Committee on Intelligence and the Committee on the Judiciary of the House of Representatives and the Select Committee on Intelligence and the Committee on the Judiciary of the Senate a report that includes—

- (A) the number of United States person queries by the Federal Bureau of Investigation of unminimized contents or noncontents acquired pursuant to section 702(a);
- (B) the number of approved queries using the Federal Bureau of Investigation's batch job technology, or successor tool;
- (C) the number of queries using the Federal Bureau of Investigation's batch job technology, or successor tool, conducted by the Federal Bureau of Investigation against information acquired pursuant to section 702(a) for which pre-approval was not obtained due to emergency circumstances;
- (D) the number of United States person queries conducted by the Federal Bureau of Investigation of unminimized contents or noncontents acquired pursuant to section 702(a) solely to retrieve evidence of a crime;
- (E) a good faith estimate of the number of United States person query terms used by the Federal Bureau of Investigation to conduct queries of unminimized contents or noncontents acquired pursuant to section 702(a) primarily to protect the United States person who is the subject of the query; and
- (F) a good faith estimate of the number of United States person query terms used by the Federal Bureau of Investigation to conduct queries of unminimized contents or noncontents acquired pursuant to section 702(a) where the United States person who is the subject of the query is a target or subject of an investigation by the Federal Bureau of Investigation.

(2) PUBLIC AVAILABILITY.—Subject to declassification review by the Attorney General and the Director of National Intelligence, each

annual report submitted pursuant to paragraph (1) shall be available to the public during the first April following the calendar year covered by the report.

(3) QUARTERLY REPORT.—Beginning on the date that is not later than 1 year after the effective date of this paragraph, the Director of the Federal Bureau of Investigation shall submit a quarterly report to the congressional intelligence committees and to the Committees on the Judiciary of the House of Representatives and of the Senate that includes the number of U.S. person queries conducted during that quarter.

(g) DEFINITIONS.—In this section:

(1) CONTENTS.—The term “contents” has the meaning given that term under section 2510 of title 18, United States Code.

(2) ELECTRONIC COMMUNICATION.—The term “electronic communication” has the meaning given that term under section 2510 of title 18, United States Code.

(3) NATIONAL SECURITY LETTER.—The term “national security letter” means a request for a report, records, or other information under—

(A) section 2709 of title 18, United States Code;

(B) section 1114(a)(5)(A) of the Right to Financial Privacy Act of 1978 (12 U.S.C. 3414(a)(5)(A));

(C) subsection (a) or (b) of section 626 of the Fair Credit Reporting Act (15 U.S.C. 1681u(a), 1681u(b)); or

(D) section 627(a) of the Fair Credit Reporting Act (15 U.S.C. 1681v(a)).

(4) UNITED STATES PERSON.—The term “United States person” means a citizen of the United States or an alien lawfully admitted for permanent residence (as defined in section 101(a) of the Immigration and Nationality Act (8 U.S.C. 1101(a))).

(5) WIRE COMMUNICATION.—The term “wire communication” has the meaning given that term under section 2510 of title 18, United States Code.

PUBLIC REPORTING BY PERSONS SUBJECT TO ORDERS

SEC. 604. [50 U.S.C. § 1874]

(a) REPORTING.—A person subject to a nondisclosure requirement accompanying an order or directive under this Act or a national security letter may, with respect to such order, directive, or national security letter, publicly report the following information using one of the following structures:

(1) A semiannual report that aggregates the number of orders, directives, or national security letters with which the person was required to comply into separate categories of—

- (A) the number of national security letters received, reported in bands of 1000 starting with 0-999;
- (B) the number of customer selectors targeted by national security letters, reported in bands of 1000 starting with 0-999;
- (C) the number of orders or directives received, combined, under this Act for contents, reported in bands of 1000 starting with 0-999;
- (D) the number of customer selectors targeted under orders or directives received, combined, under this Act for contents, reported in bands of 1000 starting with 0-999;
- (E) the number of orders received under this Act for noncontents, reported in bands of 1000 starting with 0-999; and
- (F) the number of customer selectors targeted under orders under this Act for noncontents, reported in bands of 1000 starting with 0-999, pursuant to—
 - (i) title IV;
 - (ii) title V with respect to applications described in section 501(b)(2)(B); and
 - (iii) title V with respect to applications described in section 501(b)(2)(C).

(2) A semiannual report that aggregates the number of orders, directives, or national security letters with which the person was required to comply into separate categories of—

- (A) the number of national security letters received, reported in bands of 500 starting with 0-499;
- (B) the number of customer selectors targeted by national security letters, reported in bands of 500 starting with 0-499;
- (C) the number of orders or directives received, combined, under this Act for contents, reported in bands of 500 starting with 0-499;
- (D) the number of customer selectors targeted under orders or directives received, combined, under this Act for contents, reported in bands of 500 starting with 0-499;
- (E) the number of orders received under this Act for noncontents, reported in bands of 500 starting with 0-499; and
- (F) the number of customer selectors targeted under orders received under this Act for noncontents, reported in bands of 500 starting with 0-499.

(3) A semiannual report that aggregates the number of orders, directives, or national security letters with which the person was required to comply into separate categories of—

(A) the total number of all national security process received, including all national security letters, and orders or directives under this Act, combined, reported in bands of 250 starting with 0-249; and

(B) the total number of customer selectors targeted under all national security process received, including all national security letters, and orders or directives under this Act, combined, reported in bands of 250 starting with 0-249.

(4) An annual report that aggregates the number of orders, directives, and national security letters the person was required to comply with into separate categories of—

(A) the total number of all national security process received, including all national security letters, and orders or directives under this Act, combined, reported in bands of 100 starting with 0-99; and

(B) the total number of customer selectors targeted under all national security process received, including all national security letters, and orders or directives under this Act, combined, reported in bands of 100 starting with 0-99.

(b) PERIOD OF TIME COVERED BY REPORTS.—

(1) A report described in paragraph (1) or (2) of subsection (a) shall include only information—

(A) relating to national security letters for the previous 180 days; and

(B) relating to authorities under this Act for the 180-day period of time ending on the date that is not less than 180 days prior to the date of the publication of such report, except that with respect to a platform, product, or service for which a person did not previously receive an order or directive (not including an enhancement to or iteration of an existing publicly available platform, product, or service) such report shall not include any information relating to such new order or directive until 540 days after the date on which such new order or directive is received.

(2) A report described in paragraph (3) of subsection (a) shall include only information relating to the previous 180 days.

(3) A report described in paragraph (4) of subsection (a) shall include only information for the 1-year period of time ending on the date that is not less than 1 year prior to the date of the publication of such report.

(c) OTHER FORMS OF AGREED TO PUBLICATION.—Nothing in this section prohibits the Government and any person from jointly agreeing to the publication of information referred to in this subsection in a time, form, or manner other than as described in this section.

(d) DEFINITIONS.—In this section:

(1) CONTENTS.—The term “contents” has the meaning given that term under section 2510 of title 18, United States Code.

(2) NATIONAL SECURITY LETTER.—The term “national security letter” has the meaning given that term under section 603.

TITLE VII—ADDITIONAL PROCEDURES REGARDING CERTAIN PERSONS OUTSIDE THE UNITED STATES

DEFINITIONS

SEC. 701. [50 U.S.C. § 1881]

(a) IN GENERAL.—In this title, the terms “agent of a foreign power”, “Attorney General”, “contents”, “electronic surveillance”, “foreign intelligence information”, “foreign power”, “person”, “United States”, and “United States person” have the meanings given such terms in section 101, except as specifically provided in this title.

(b) ADDITIONAL DEFINITIONS.—In this title:

(1) CONGRESSIONAL INTELLIGENCE COMMITTEES.—The term “congressional intelligence committees” means—

(A) the Select Committee on Intelligence of the Senate; and

(B) the Permanent Select Committee on Intelligence of the House of Representatives.

(2) FOREIGN INTELLIGENCE SURVEILLANCE COURT; COURT.—The terms “Foreign Intelligence Surveillance Court” and “Court” mean the court established under section 103(a).

(3) FOREIGN INTELLIGENCE SURVEILLANCE COURT OF REVIEW; COURT OF REVIEW.—The terms “Foreign Intelligence Surveillance Court of Review” and “Court of Review” mean the court established under section 103(b).

(4) ELECTRONIC COMMUNICATION SERVICE PROVIDER.—The term “electronic communication service provider” means—

(A) a telecommunications carrier, as that term is defined in section 3 of the Communications Act of 1934 (47 U.S.C. 153);

(B) a provider of electronic communication service, as that term is defined in section 2510 of title 18, United States Code;

(C) a provider of a remote computing service, as that term is defined in section 2711 of title 18, United States Code;

(D) any other communication service provider who has access to wire or electronic communications either as such communications are transmitted or as such communications are stored;

(E) any other service provider who has access to equipment that is being or may be used to transmit or store wire or electronic communications, but not including any entity that serves primarily as—

(i) a public accommodation facility, as that term is defined in section 501(4);

(ii) a dwelling, as that term is defined in section 802 of the Fair Housing Act (42 U.S.C. 3602);

(iii) a community facility, as that term is defined in section 315 of the Defense Housing and Community Facilities and Services Act of 1951 (42 U.S.C. 1592n);
or

(iv) a food service establishment, as that term is defined in section 281 of the Agricultural Marketing Act of 1946 (7 U.S.C. 1638); or

(F) an officer, employee, custodian, or agent of an entity described in subparagraph (A), (B), (C), (D), or (E).

(5) INTELLIGENCE COMMUNITY.—The term “intelligence community” has the meaning given the term in section 3(4) of the National Security Act of 1947 (50 U.S.C. [3003(4)]).

PROCEDURES FOR TARGETING CERTAIN PERSONS OUTSIDE THE UNITED STATES OTHER THAN UNITED STATES PERSONS

SEC. 702. [50 U.S.C. § 1881a]

(a) AUTHORIZATION.—Notwithstanding any other provision of law, upon the issuance of an order in accordance with subsection (j)(3) or a determination under subsection (c)(2), the Attorney General and the Director of National Intelligence may authorize jointly, for a period of up to 1 year from the effective date of the authorization, the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information.

(b) LIMITATIONS.—An acquisition authorized under subsection (a)—

(1) may not intentionally target any person known at the time of acquisition to be located in the United States;

(2) may not intentionally target a person reasonably believed to be located outside the United States if the purpose of such acquisition is to target a particular, known person reasonably believed to be in the United States;

(3) may not intentionally target a United States person reasonably believed to be located outside the United States;

(4) may not intentionally acquire any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States;

(5) may not intentionally acquire communications that contain a reference to, but are not to or from, a target of an acquisition authorized under subsection (a); and

(6) shall be conducted in a manner consistent with the fourth amendment to the Constitution of the United States.

(c) CONDUCT OF ACQUISITION.—

(1) IN GENERAL.—An acquisition authorized under subsection (a) shall be conducted only in accordance with—

(A) the targeting and minimization procedures adopted in accordance with subsections (d) and (e); and

(B) upon submission of a certification in accordance with subsection (h), such certification.

(2) DETERMINATION.—A determination under this paragraph and for purposes of subsection (a) is a determination by the Attorney General and the Director of National Intelligence that exigent circumstances exist because, without immediate implementation of an authorization under subsection (a), intelligence important to the national security of the United States may be lost or not timely acquired and time does not permit the issuance of an order pursuant to subsection (j)(3) prior to the implementation of such authorization.

(3) TIMING OF DETERMINATION.—The Attorney General and the Director of National Intelligence may make the determination under paragraph (2)—

(A) before the submission of a certification in accordance with subsection (h); or

(B) by amending a certification pursuant to subsection (j)(1)(C) at any time during which judicial review under subsection (j) of such certification is pending.

(4) CONSTRUCTION.—Nothing in title I shall be construed to require an application for a court order under such title for an acquisition that is targeted in accordance with this section at a person reasonably believed to be located outside the United States.

(d) TARGETING PROCEDURES.—

(1) REQUIREMENT TO ADOPT.—The Attorney General, in consultation with the Director of National Intelligence, shall adopt targeting procedures that are reasonably designed to—

(A) ensure that any acquisition authorized under subsection (a) is limited to targeting persons reasonably believed to be located outside the United States; and

(B) prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States.

(2) JUDICIAL REVIEW.—The procedures adopted in accordance with paragraph (1) shall be subject to judicial review pursuant to subsection (j).

(e) MINIMIZATION PROCEDURES.—

(1) REQUIREMENT TO ADOPT.—The Attorney General, in consultation with the Director of National Intelligence, shall adopt minimization procedures that meet the definition of minimization procedures under section 101(h) or section 301(4), as appropriate, for acquisitions authorized under subsection (a).

(2) JUDICIAL REVIEW.—The minimization procedures adopted in accordance with paragraph (1) shall be subject to judicial review pursuant to subsection (j).

(3) PUBLICATION.—The Director of National Intelligence, in consultation with the Attorney General, shall—

(A) conduct a declassification review of any minimization procedures adopted or amended in accordance with paragraph (1); and

(B) consistent with such review, and not later than 180 days after conducting such review, make such minimization procedures publicly available to the greatest extent practicable, which may be in redacted form.

(f) QUERIES.—

(1) PROCEDURES REQUIRED.—

(A) REQUIREMENT TO ADOPT.—The Attorney General, in consultation with the Director of National Intelligence, shall adopt querying procedures consistent with the requirements of the fourth amendment to the Constitution of the United States for information collected pursuant to an authorization under subsection (a).

(B) RECORD OF UNITED STATES PERSON QUERY TERMS.—The Attorney General, in consultation with the Director of National

Intelligence, shall ensure that the procedures adopted under subparagraph (A) include a technical procedure whereby a record is kept of each United States person query term used for a query.

(C) JUDICIAL REVIEW.—The procedures adopted in accordance with subparagraph (A) shall be subject to judicial review pursuant to subsection (j).

(2) ACCESS TO RESULTS OF CERTAIN QUERIES CONDUCTED BY FBI.—

(A) COURT ORDER REQUIRED FOR FBI REVIEW OF CERTAIN QUERY RESULTS IN CRIMINAL INVESTIGATIONS UNRELATED TO NATIONAL SECURITY.—Except as provided by subparagraph (E), in connection with a predicated criminal investigation opened by the Federal Bureau of Investigation that does not relate to the national security of the United States, the Federal Bureau of Investigation may not access the contents of communications acquired under subsection (a) that were retrieved pursuant to a query made using a United States person query term that was not designed to find and extract foreign intelligence information unless—

- (i) the Federal Bureau of Investigation applies for an order of the Court under subparagraph (C); and
- (ii) the Court enters an order under subparagraph (D) approving such application.

(B) JURISDICTION.—The Court shall have jurisdiction to review an application and to enter an order approving the access described in subparagraph (A).

(C) APPLICATION.—Each application for an order under this paragraph shall be made by a Federal officer in writing upon oath or affirmation to a judge having jurisdiction under subparagraph (B). Each application shall require the approval of the Attorney General based upon the finding of the Attorney General that the application satisfies the criteria and requirements of such application, as set forth in this paragraph, and shall include—

- (i) the identity of the Federal officer making the application; and
- (ii) an affidavit or other information containing a statement of the facts and circumstances relied upon by the applicant to justify the belief of the applicant that the contents of communications described in subparagraph

(A) covered by the application would provide evidence of—

- (I) criminal activity;
- (II) contraband, fruits of a crime, or other items illegally possessed by a third party; or
- (III) property designed for use, intended for use, or used in committing a crime.

(D) ORDER.—Upon an application made pursuant to subparagraph (C), the Court shall enter an order approving the accessing of the contents of communications described in subparagraph (A) covered by the application if the Court finds probable cause to believe that such contents would provide any of the evidence described in subparagraph (C)(ii).

(E) EXCEPTION.—The requirement for an order of the Court under subparagraph (A) to access the contents of communications described in such subparagraph shall not apply with respect to a query if the Federal Bureau of Investigation determines there is a reasonable belief that such contents could assist in mitigating or eliminating a threat to life or serious bodily harm.

(F) RULE OF CONSTRUCTION.—Nothing in this paragraph may be construed as—

- (i) limiting the authority of the Federal Bureau of Investigation to conduct lawful queries of information acquired under subsection (a);
- (ii) limiting the authority of the Federal Bureau of Investigation to review, without a court order, the results of any query of information acquired under subsection (a) that was reasonably designed to find and extract foreign intelligence information, regardless of whether such foreign intelligence information could also be considered evidence of a crime; or
- (iii) prohibiting or otherwise limiting the ability of the Federal Bureau of Investigation to access the results of queries conducted when evaluating whether to open an assessment or predicated investigation relating to the national security of the United States.

(3) RESTRICTIONS IMPOSED ON FEDERAL BUREAU OF INVESTIGATION.—

(A) LIMITS ON AUTHORIZATIONS OF UNITED STATES PERSON QUERIES.—

(i) **IN GENERAL.**—Federal Bureau of Investigation personnel must obtain prior approval from a Federal Bureau of Investigation supervisor (or employee of equivalent or greater rank) or attorney who is authorized to access unminimized contents or noncontents obtained through acquisitions authorized under subsection (a) for any query of such unminimized contents or noncontents made using a United States person query term.

(ii) **EXCEPTION.**—A United States person query to be conducted by the Federal Bureau of Investigation of unminimized contents or noncontents obtained through acquisitions authorized under subsection (a) using a United States person query term may be conducted without obtaining prior approval as specified in clause (i) only if the person conducting the United States person query has a reasonable belief that conducting the query could assist in mitigating or eliminating a threat to life or serious bodily harm.

(B) NOTIFICATION REQUIREMENT FOR CERTAIN FBI QUERIES

(i) **REQUIREMENT** - The Director of the Federal Bureau of Investigation shall promptly notify appropriate congressional leadership of any query conducted by the Federal Bureau of Investigation using a query term that is reasonably believed to be the name or other personally identifying information of a member of Congress, and shall also notify the member who is the subject of such query.

(ii) **APPROPRIATE CONGRESSIONAL LEADERSHIP DEFINED.** In this subparagraph, the term “appropriate congressional leadership” means the following:

- (I) The chairs and ranking minority members of the congressional intelligence committees.
- (II) The Speaker and minority leader of the House of Representatives.
- (III) The majority and minority leaders of the Senate.

(iii) **NATIONAL SECURITY CONSIDERATIONS** In submitting a notification under clause (i), the Director shall give due regard to the protection of classified information, sources and methods, and national security.

(iv) **WAIVER**

(I) IN GENERAL The Director may waive a notification required under clause (i) if the Director determines such notification would impede an ongoing national security or law enforcement investigation.

(II) TERMINATION A waiver under subclause (I) shall terminate on the date the Director determines the relevant notification would not impede the relevant national security or law enforcement investigation or on the date that such investigation ends, whichever is earlier.

(C) CONSENT REQUIRED FOR FBI TO CONDUCT CERTAIN
QUERIES FOR PURPOSE OF DEFENSIVE BRIEFING

(i) CONSENT REQUIRED The Federal Bureau of Investigation may not, for the exclusive purpose of supplementing the contents of a briefing on the defense against a counterintelligence threat to a member of Congress, conduct a query using a query term that is the name or restricted personal information (as such term is defined in section 119 of title 18) of that member unless—

(I) the member provides consent to the use of the query term; or

(II) the Deputy Director of the Federal Bureau of Investigation determines that exigent circumstances exist sufficient to justify the conduct of such query.

(ii) NOTIFICATION

(I) NOTIFICATION OF CONSENT SOUGHT Not later than three business days after submitting a request for consent from a member of Congress under clause (i), the Director of the Federal Bureau of Investigation shall notify the appropriate congressional leadership, regardless of whether the member provided such consent.

(II) NOTIFICATION OF EXCEPTION USED Not later than three business days after the conduct of a query under clause (i) without consent on the basis of the existence of exigent circumstances determined under subclause (II) of such clause, the Director of the Federal

Bureau of Investigation shall notify the appropriate congressional leadership.

(iii) **RULE OF CONSTRUCTION** Nothing in this subparagraph may be construed as—

(I) applying to matters outside of the scope of the briefing on the defense against a counterintelligence threat to be provided or supplemented under clause (i); or

(II) limiting the lawful investigative activities of the Federal Bureau of Investigation other than supplementing the contents of a briefing on the defense against a counterintelligence threat to a member of Congress.

(iv) **APPROPRIATE CONGRESSIONAL LEADERSHIP**

DEFINED In this subparagraph, the term “appropriate congressional leadership” means the following:

(I) The chairs and ranking minority members of the congressional intelligence committees.

(II) The Speaker and minority leader of the House of Representatives.

(III) The majority and minority leaders of the Senate.

(D) **QUERYING PROCEDURES APPLICABLE TO FEDERAL BUREAU OF INVESTIGATION** For any procedures adopted under paragraph

(1) applicable to the Federal Bureau of Investigation, the Attorney General, in consultation with the Director of National Intelligence, shall include the following requirements:

(i) **TRAINING** A requirement that, prior to conducting any query, personnel of the Federal Bureau of Investigation successfully complete training on the querying procedures on an annual basis.

(ii) **ADDITIONAL PRIOR APPROVALS FOR SENSITIVE QUERIES** A requirement that, absent exigent circumstances, prior to conducting certain queries, personnel of the Federal Bureau of Investigation receive approval, at minimum, as follows:

(I) Approval from the Deputy Director of the Federal Bureau of Investigation if the query uses a query term reasonably believed to identify a United States elected official, an appointee of the President or a State governor, a United States

political candidate, a United States political organization or a United States person prominent in such organization, or a United States media organization or a United States person who is a member of such organization.

(II) Approval from an attorney of the Federal Bureau of Investigation if the query uses a query term reasonably believed to identify a United States religious organization or a United States person who is prominent in such organization.

(III) Approval from an attorney of the Federal Bureau of Investigation if such conduct involves batch job technology (or successor tool).

(iii) **PRIOR WRITTEN JUSTIFICATION** A requirement that, prior to conducting a query using a United States person query term, personnel of the Federal Bureau of Investigation provide a written statement of the specific factual basis to support the reasonable belief that such query meets the standards required by the procedures adopted under paragraph (1). For each United States person query, the Federal Bureau of Investigation shall keep a record of the query term, the date of the conduct of the query, the identifier of the personnel conducting the query, and such written statement.

(iv) **STORAGE OF CERTAIN CONTENTS AND NONCONTENTS** Any system of the Federal Bureau of Investigation that stores unminimized contents or noncontents obtained through acquisitions authorized under subsection (a) together with contents or noncontents obtained through other lawful means shall be configured in a manner that—

- (I) requires personnel of the Federal Bureau of Investigation to affirmatively elect to include such unminimized contents or noncontents obtained through acquisitions authorized under subsection (a) when running a query; or
- (II) includes other controls reasonably expected to prevent inadvertent queries of such unminimized contents or noncontents.

(v) **WAIVER AUTHORITY FOR FOREIGN INTELLIGENCE SURVEILLANCE COURT** If the Foreign Intelligence

Surveillance Court finds that the procedures adopted under paragraph (1) include measures that are reasonably expected to result in similar compliance outcomes as the measures specified in clauses (i) through (iv) of this subparagraph, the Foreign Intelligence Surveillance Court may waive one or more of the requirements specified in such clauses.

(vi) PROHIBITION ON POLITICAL APPOINTEES WITHIN THE PROCESS TO APPROVE FEDERAL BUREAU OF INVESTIGATION QUERIES The procedures shall prohibit any political personnel, such as those classified by the Office of Personnel Management as Presidential Appointment with Senate Confirmation, Presidential Appointment (without Senate Confirmation), Noncareer Senior Executive Service Appointment, or Schedule C Excepted Appointment, from inclusion in the Federal Bureau of Investigation's prior approval process under clause (ii).

(4) MINIMUM ACCOUNTABILITY STANDARDS The Director of the Federal Bureau of Investigation shall issue minimum accountability standards that set forth escalating consequences for noncompliant querying of United States person terms within the contents of communications that were acquired under this section. Such standards shall include, at minimum, the following:

(A) Zero tolerance for willful misconduct.

(B) Escalating consequences for unintentional noncompliance, including the threshold for mandatory revocation of access to query information acquired under this section.

(C) Consequences for supervisors who oversee users that engage in noncompliant queries.

(5) DEFINITIONS.—In this subsection:

(A) The term “contents” has the meaning given that term in section 2510(8) of title 18, United States Code.

(B) The term “query” means the use of one or more terms to retrieve the unminimized contents or noncontents located in electronic and data storage systems of communications of or concerning United States persons obtained through acquisitions authorized under subsection (a).

(6) VETTING OF NON-UNITED STATES PERSONS.—For any procedures for one or more agencies adopted under paragraph (1)(A), the Attorney General, in consultation with the Director of National Intelligence, shall

ensure that the procedures enable the vetting of all non-United States persons who are being processed for travel to the United States using terms that do not qualify as United States person query terms under this Act.

(g) GUIDELINES FOR COMPLIANCE WITH LIMITATIONS.—

(1) REQUIREMENT TO ADOPT.—The Attorney General, in consultation with the Director of National Intelligence, shall adopt guidelines to ensure—

- (A) compliance with the limitations in subsection (b); and
- (B) that an application for a court order is filed as required by this Act.

(2) SUBMISSION OF GUIDELINES.—The Attorney General shall provide the guidelines adopted in accordance with paragraph (1) to—

- (A) the congressional intelligence committees;
- (B) the Committees on the Judiciary of the Senate and the House of Representatives; and
- (C) the Foreign Intelligence Surveillance Court.

(h) CERTIFICATION.—

(1) IN GENERAL.—

(A) REQUIREMENT.—Subject to subparagraph (B), prior to the implementation of an authorization under subsection (a), the Attorney General and the Director of National Intelligence shall provide to the Foreign Intelligence Surveillance Court a written certification and any supporting affidavit, under oath and under seal, in accordance with this subsection.

(B) EXCEPTION.—If the Attorney General and the Director of National Intelligence make a determination under subsection (c)(2) and time does not permit the submission of a certification under this subsection prior to the implementation of an authorization under subsection (a), the Attorney General and the Director of National Intelligence shall submit to the Court a certification for such authorization as soon as practicable but in no event later than 7 days after such determination is made.

(2) REQUIREMENTS.—A certification made under this subsection shall—

(A) attest that—

- (i) there are targeting procedures in place that have been approved, have been submitted for approval, or will be submitted with the certification for approval by the Foreign Intelligence Surveillance Court that are reasonably designed to—

- (I) ensure that an acquisition authorized under subsection (a) is limited to targeting persons reasonably believed to be located outside the United States; and
- (II) prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States;
- (ii) the minimization procedures to be used with respect to such acquisition—
 - (I) meet the definition of minimization procedures under section 101(h) or 301(4), as appropriate; and
 - (II) have been approved, have been submitted for approval, or will be submitted with the certification for approval by the Foreign Intelligence Surveillance Court;
- (iii) guidelines have been adopted in accordance with subsection (g) to ensure compliance with the limitations in subsection (b) and to ensure that an application for a court order is filed as required by this Act;
- (iv) the procedures and guidelines referred to in clauses (i), (ii), and (iii) are consistent with the requirements of the fourth amendment to the Constitution of the United States;
- (v) a significant purpose of the acquisition is to obtain foreign intelligence information;
- (vi) the acquisition involves obtaining foreign intelligence information from or with the assistance of an electronic communication service provider; and
- (vii) the acquisition complies with the limitations in subsection (b);
- (B) include the procedures adopted in accordance with subsections (d) and (e);
- (C) be supported, as appropriate, by the affidavit of any appropriate official in the area of national security who is—
 - (i) appointed by the President, by and with the advice and consent of the Senate; or
 - (ii) the head of an element of the intelligence community;
- (D) include—

(i) an effective date for the authorization that is at least 30 days after the submission of the written certification to the court; or

(ii) if the acquisition has begun or the effective date is less than 30 days after the submission of the written certification to the court, the date the acquisition began or the effective date for the acquisition; and

(E) if the Attorney General and the Director of National Intelligence make a determination under subsection (c)(2), include a statement that such determination has been made.

(3) CHANGE IN EFFECTIVE DATE.—The Attorney General and the Director of National Intelligence may advance or delay the effective date referred to in paragraph (2)(D) by submitting an amended certification in accordance with subsection (j)(1)(C) to the Foreign Intelligence Surveillance Court for review pursuant to subsection (i).

(4) LIMITATION.—A certification made under this subsection is not required to identify the specific facilities, places, premises, or property at which an acquisition authorized under subsection (a) will be directed or conducted.

(5) MAINTENANCE OF CERTIFICATION.—The Attorney General or a designee of the Attorney General shall maintain a copy of a certification made under this subsection.

(6) REVIEW.—A certification submitted in accordance with this subsection shall be subject to judicial review pursuant to subsection (j).

(i) DIRECTIVES AND JUDICIAL REVIEW OF DIRECTIVES.—

(1) AUTHORITY.—With respect to an acquisition authorized under subsection (a), the Attorney General and the Director of National Intelligence may direct, in writing, an electronic communication service provider to—

(A) immediately provide the Government with all information, facilities, or assistance necessary to accomplish the acquisition in a manner that will protect the secrecy of the acquisition and produce a minimum of interference with the services that such electronic communication service provider is providing to the target of the acquisition; and

(B) maintain under security procedures approved by the Attorney General and the Director of National Intelligence any records concerning the acquisition or the aid furnished that such electronic communication service provider wishes to maintain.

(2) COMPENSATION.—The Government shall compensate, at the prevailing rate, an electronic communication service provider for

providing information, facilities, or assistance in accordance with a directive issued pursuant to paragraph (1).

(3) **RELEASE FROM LIABILITY.**—No cause of action shall lie in any court against any electronic communication service provider for providing any information, facilities, or assistance in accordance with a directive issued pursuant to paragraph (1).

(4) **CHALLENGING OF DIRECTIVES.**—

(A) **AUTHORITY TO CHALLENGE.**—An electronic communication service provider receiving a directive issued pursuant to paragraph (1) may file a petition to modify or set aside such directive with the Foreign Intelligence Surveillance Court, which shall have jurisdiction to review such petition.

(B) **ASSIGNMENT.**—The presiding judge of the Court shall assign a petition filed under subparagraph (A) to 1 of the judges serving in the pool established under section 103(e)(1) not later than 24 hours after the filing of such petition.

(C) **STANDARDS FOR REVIEW.**—A judge considering a petition filed under subparagraph (A) may grant such petition only if the judge finds that the directive does not meet the requirements of this section, or is otherwise unlawful.

(D) **PROCEDURES FOR INITIAL REVIEW.**—A judge shall conduct an initial review of a petition filed under subparagraph (A) not later than 5 days after being assigned such petition. If the judge determines that such petition does not consist of claims, defenses, or other legal contentions that are warranted by existing law or by a nonfrivolous argument for extending, modifying, or reversing existing law or for establishing new law, the judge shall immediately deny such petition and affirm the directive or any part of the directive that is the subject of such petition and order the recipient to comply with the directive or any part of it. Upon making a determination under this subparagraph or promptly thereafter, the judge shall provide a written statement for the record of the reasons for such determination.

(E) **PROCEDURES FOR PLENARY REVIEW.**—If a judge determines that a petition filed under subparagraph (A) requires plenary review, the judge shall affirm, modify, or set aside the directive that is the subject of such petition not later than 30 days after being assigned such petition. If the judge does not set aside the directive, the judge shall immediately affirm or affirm with modifications the directive, and order the recipient to comply

with the directive in its entirety or as modified. The judge shall provide a written statement for the record of the reasons for a determination under this subparagraph.

(F) CONTINUED EFFECT.—Any directive not explicitly modified or set aside under this paragraph shall remain in full effect.

(G) CONTEMPT OF COURT.—Failure to obey an order issued under this paragraph may be punished by the Court as contempt of court.

(5) ENFORCEMENT OF DIRECTIVES.—

(A) ORDER TO COMPEL.—If an electronic communication service provider fails to comply with a directive issued pursuant to paragraph (1), the Attorney General may file a petition for an order to compel the electronic communication service provider to comply with the directive with the Foreign Intelligence Surveillance Court, which shall have jurisdiction to review such petition.

(B) ASSIGNMENT.—The presiding judge of the Court shall assign a petition filed under subparagraph (A) to 1 of the judges serving in the pool established under section 103(e)(1) of this title not later than 24 hours after the filing of such petition.

(C) PROCEDURES FOR REVIEW.—A judge considering a petition filed under subparagraph (A) shall, not later than 30 days after being assigned such petition, issue an order requiring the electronic communication service provider to comply with the directive or any part of it, as issued or as modified, if the judge finds that the directive meets the requirements of this section and is otherwise lawful. The judge shall provide a written statement for the record of the reasons for a determination under this paragraph.

(D) CONTEMPT OF COURT.—Failure to obey an order issued under this paragraph may be punished by the Court as contempt of court.

(E) PROCESS.—Any process under this paragraph may be served in any judicial district in which the electronic communication service provider may be found.

(6) APPEAL.—

(A) APPEAL TO THE COURT OF REVIEW.—The Government or an electronic communication service provider receiving a directive issued pursuant to paragraph (1) may file a petition with the Foreign Intelligence Surveillance Court of Review for review of a decision issued pursuant to paragraph (4) or (5). The Court of

Review shall have jurisdiction to consider such petition and shall provide a written statement for the record of the reasons for a decision under this subparagraph.

(B) CERTIORARI TO THE SUPREME COURT.—The Government or an electronic communication service provider receiving a directive issued pursuant to paragraph (1) may file a petition for a writ of certiorari for review of a decision of the Court of Review issued under subparagraph (A). The record for such review shall be transmitted under seal to the Supreme Court of the United States, which shall have jurisdiction to review such decision.

(j) JUDICIAL REVIEW OF CERTIFICATIONS AND PROCEDURES.—

(1) IN GENERAL.—

(A) REVIEW BY THE FOREIGN INTELLIGENCE SURVEILLANCE COURT.—The Foreign Intelligence Surveillance Court shall have jurisdiction to review a certification submitted in accordance with subsection (g) and the targeting, minimization, and querying procedures adopted in accordance with subsections (d), (e), and (f)(1), and amendments to such certification or such procedures.

(B) TIME PERIOD FOR REVIEW.—The Court shall review a certification submitted in accordance with subsection (g) and the targeting, minimization, and querying procedures adopted in accordance with subsections (d), (e), and (f)(1) and shall complete such review and issue an order under paragraph (3) not later than 30 days after the date on which such certification and such procedures are submitted.

(C) AMENDMENTS.—The Attorney General and the Director of National Intelligence may amend a certification submitted in accordance with subsection (g) or the targeting, minimization, and querying procedures adopted in accordance with subsections (d), (e), and (f)(1) as necessary at any time, including if the Court is conducting or has completed review of such certification or such procedures, and shall submit the amended certification or amended procedures to the Court not later than 7 days after amending such certification or such procedures. The Court shall review any amendment under this subparagraph under the procedures set forth in this subsection. The Attorney General and the Director of National Intelligence may authorize the use of an amended certification or amended procedures

pending the Court's review of such amended certification or amended procedures.

(2) REVIEW.—The Court shall review the following:

(A) CERTIFICATION.—A certification submitted in accordance with subsection (h) to determine whether the certification contains all the required elements.

(B) TARGETING PROCEDURES.—The targeting procedures adopted in accordance with subsection (d) to assess whether the procedures are reasonably designed to—

(i) ensure that an acquisition authorized under subsection (a) is limited to targeting persons reasonably believed to be located outside the United States; and

(ii) prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States.

(C) MINIMIZATION PROCEDURES.—The minimization procedures adopted in accordance with subsection (e) to assess whether such procedures meet the definition of minimization procedures under section 101(h) or section 301(4), as appropriate.

(D) QUERYING PROCEDURES.—The querying procedures adopted in accordance with subsection (f)(1) to assess whether such procedures comply with the requirements of such subsection.

(3) ORDERS.—

(A) APPROVAL.—If the Court finds that a certification submitted in accordance with subsection (h) contains all the required elements and that the targeting, minimization, and querying procedures adopted in accordance with subsections (d), (e), and (f)(1) are consistent with the requirements of those subsections and with the fourth amendment to the Constitution of the United States, the Court shall enter an order approving the certification and the use, or continued use in the case of an acquisition authorized pursuant to a determination under subsection (c)(2), of the procedures for the acquisition.

(B) CORRECTION OF DEFICIENCIES.—If the Court finds that a certification submitted in accordance with subsection (h) does not contain all the required elements, or that the procedures adopted in accordance with subsections (d), (e), and (f)(1) are not consistent with the requirements of those subsections or the

fourth amendment to the Constitution of the United States, the Court shall issue an order directing the Government to, at the Government's election and to the extent required by the Court's order—

- (i) correct any deficiency identified by the Court's order not later than 30 days after the date on which the Court issues the order; or
- (ii) cease, or not begin, the implementation of the authorization for which such certification was submitted.

(C) REQUIREMENT FOR WRITTEN STATEMENT.—In support of an order under this subsection, the Court shall provide, simultaneously with the order, for the record a written statement of the reasons for the order.

(D) LIMITATION ON USE OF INFORMATION.—

(i) IN GENERAL.—Except as provided in clause (ii), if the Court orders a correction of a deficiency in a certification or procedures under subparagraph (B), no information obtained or evidence derived pursuant to the part of the certification or procedures that has been identified by the Court as deficient concerning any United States person shall be received in evidence or otherwise disclosed in any trial, hearing, or other proceeding in or before any court, grand jury, department, office, agency, regulatory body, legislative committee, or other authority of the United States, a State, or political subdivision thereof, and no information concerning any United States person acquired pursuant to such part of such certification or procedures shall subsequently be used or disclosed in any other manner by Federal officers or employees without the consent of the United States person, except with the approval of the Attorney General if the information indicates a threat of death or serious bodily harm to any person.

(ii) EXCEPTION.—If the Government corrects any deficiency identified by the order of the Court under subparagraph (B), the Court may permit the use or disclosure of information obtained before the date of the correction under such minimization procedures as the Court may approve for purposes of this clause.

(4) APPEAL.—

(A) APPEAL TO THE COURT OF REVIEW.—The Government may file a petition with the Foreign Intelligence Surveillance Court of Review for review of an order under this subsection. The Court of Review shall have jurisdiction to consider such petition. For any decision under this subparagraph affirming, reversing, or modifying an order of the Foreign Intelligence Surveillance Court, the Court of Review shall provide for the record a written statement of the reasons for the decision.

(B) CONTINUATION OF ACQUISITION PENDING REHEARING OR APPEAL.—Any acquisition affected by an order under paragraph (3)(B) may continue—

- (i) during the pendency of any rehearing of the order by the Court en banc; and
- (ii) if the Government files a petition for review of an order under this section, until the Court of Review enters an order under subparagraph (C).

(C) IMPLEMENTATION PENDING APPEAL.—Not later than 60 days after the filing of a petition for review of an order under paragraph (3)(B) directing the correction of a deficiency, the Court of Review shall determine, and enter a corresponding order regarding, whether all or any part of the correction order, as issued or modified, shall be implemented during the pendency of the review.

(D) CERTIORARI TO THE SUPREME COURT.—The Government may file a petition for a writ of certiorari for review of a decision of the Court of Review issued under subparagraph (A). The record for such review shall be transmitted under seal to the Supreme Court of the United States, which shall have jurisdiction to review such decision.

(5) SCHEDULE.—

(A) REAUTHORIZATION OF AUTHORIZATIONS IN EFFECT.—If the Attorney General and the Director of National Intelligence seek to reauthorize or replace an authorization issued under subsection (a), the Attorney General and the Director of National Intelligence shall, to the extent practicable, submit to the Court the certification prepared in accordance with subsection (h) and the procedures adopted in accordance with subsections (d), (e), and (f)(1) at least 30 days prior to the expiration of such authorization.

(B) REAUTHORIZATION OF ORDERS, AUTHORIZATIONS, AND DIRECTIVES.—If the Attorney General and the Director of National Intelligence seek to reauthorize or replace an authorization issued under subsection (a) by filing a certification pursuant to subparagraph (A), that authorization, and any directives issued thereunder and any order related thereto, shall remain in effect, notwithstanding the expiration provided for in subsection (a), until the Court issues an order with respect to such certification under paragraph (3) at which time the provisions of that paragraph and paragraph (4) shall apply with respect to such certification.

(k) JUDICIAL PROCEEDINGS.—

(1) EXPEDITED JUDICIAL PROCEEDINGS.—Judicial proceedings under this section shall be conducted as expeditiously as possible.

(2) TIME LIMITS.—A time limit for a judicial decision in this section shall apply unless the Court, the Court of Review, or any judge of either the Court or the Court of Review, by order for reasons stated, extends that time as necessary for good cause in a manner consistent with national security.

(l) MAINTENANCE AND SECURITY OF RECORDS AND PROCEEDINGS.—

(1) STANDARDS.—The Foreign Intelligence Surveillance Court shall maintain a record of a proceeding under this section, including petitions, appeals, orders, and statements of reasons for a decision, under security measures adopted by the Chief Justice of the United States, in consultation with the Attorney General and the Director of National Intelligence.

(2) FILING AND REVIEW.—All petitions under this section shall be filed under seal. In any proceedings under this section, the Court shall, upon request of the Government, review *ex parte* and *in camera* any Government submission, or portions of a submission, which may include classified information.

(3) RETENTION OF RECORDS.—The Attorney General and the Director of National Intelligence shall retain a directive or an order issued under this section for a period of not less than 10 years from the date on which such directive or such order is issued.

(m) ASSESSMENTS AND REVIEWS.—

(1) SEMIANNUAL ASSESSMENT.—Not less frequently than once every 6 months, the Attorney General and Director of National Intelligence shall assess compliance with the targeting, minimization, and querying procedures adopted in accordance with subsections (d), (e), and (f)(1)

and the guidelines adopted in accordance with subsection (g) and shall submit each assessment to—

(A) the Foreign Intelligence Surveillance Court; and

(B) consistent with the Rules of the House of Representatives, the Standing Rules of the Senate, and Senate Resolution 400 of the 94th Congress or any successor Senate resolution—

(i) the congressional intelligence committees; and

(ii) the Committees on the Judiciary of the House of Representatives and the Senate.

(2) AGENCY ASSESSMENT.—The Inspector General of the Department of Justice and the Inspector General of each element of the intelligence community authorized to acquire foreign intelligence information under subsection (a), with respect to the department or element of such Inspector General—

(A) are authorized to review compliance with the targeting, minimization, and querying procedures adopted in accordance with subsections (d), (e), and (f)(1) and the guidelines adopted in accordance with subsection (g);

(B) with respect to acquisitions authorized under subsection (a), shall review the number of disseminated intelligence reports containing a reference to a United States-person identity and the number of United States-person identities subsequently disseminated by the element concerned in response to requests for identities that were not referred to by name or title in the original reporting;

(C) with respect to acquisitions authorized under subsection (a), shall review the number of targets that were later determined to be located in the United States and, to the extent possible, whether communications of such targets were reviewed; and

(D) shall provide each such review to—

(i) the Attorney General;

(ii) the Director of National Intelligence; and

(iii) consistent with the Rules of the House of Representatives, the Standing Rules of the Senate, and Senate Resolution 400 of the 94th Congress or any successor Senate resolution—

(I) the congressional intelligence committees; and

(II) the Committees on the Judiciary of the House of Representatives and the Senate.

(3) ANNUAL REVIEW.—

(A) REQUIREMENT TO CONDUCT.—The head of each element of the intelligence community conducting an acquisition authorized under subsection (a) shall conduct an annual review to determine whether there is reason to believe that foreign intelligence information has been or will be obtained from the acquisition. The annual review shall provide, with respect to acquisitions authorized under subsection (a)—

- (i) an accounting of the number of disseminated intelligence reports containing a reference to a United States-person identity;
- (ii) an accounting of the number of United States-person identities subsequently disseminated by that element in response to requests for identities that were not referred to by name or title in the original reporting;
- (iii) the number of targets that were later determined to be located in the United States and, to the extent possible, whether communications of such targets were reviewed; and
- (iv) a description of any procedures developed by the head of such element of the intelligence community and approved by the Director of National Intelligence to assess, in a manner consistent with national security, operational requirements and the privacy interests of United States persons, the extent to which the acquisitions authorized under subsection (a) acquire the communications of United States persons, and the results of any such assessment.

(B) USE OF REVIEW.—The head of each element of the intelligence community that conducts an annual review under subparagraph (A) shall use each such review to evaluate the adequacy of the minimization procedures utilized by such element and, as appropriate, the application of the minimization procedures to a particular acquisition authorized under subsection (a).

(C) PROVISION OF REVIEW.—The head of each element of the intelligence community that conducts an annual review under subparagraph (A) shall provide such review to—

- (i) the Foreign Intelligence Surveillance Court;
- (ii) the Attorney General;
- (iii) the Director of National Intelligence; and

(iv) consistent with the Rules of the House of Representatives, the Standing Rules of the Senate, and Senate Resolution 400 of the 94th Congress or any successor Senate resolution—

- (I) the congressional intelligence committees; and
- (II) the Committees on the Judiciary of the House of Representatives and the Senate.

(n) RESTRICTION ON CERTAIN INFORMATION AVAILABLE TO FEDERAL BUREAU OF INVESTIGATION.—

(1) RESTRICTION.—The Federal Bureau of Investigation may not ingest unminimized information acquired under this section into its analytic repositories unless the targeted person is relevant to an existing, open, predicated full national security investigation by the Federal Bureau of Investigation.

(2) EXCEPTION FOR EXIGENT CIRCUMSTANCES.—Paragraph (1) does not apply if the Director of the Federal Bureau of Investigation decides it is necessary due to exigent circumstances and provides notification within three business days to the congressional intelligence committees, the Speaker and minority leader of the House of Representatives, and the majority and minority leaders of the Senate.

(3) EXCEPTION FOR ASSISTANCE TO OTHER AGENCIES.— Paragraph (1) does not apply where the Federal Bureau of Investigation has agreed to provide technical, analytical, or linguistic assistance at the request of another Federal agency.

CERTAIN ACQUISITIONS INSIDE THE UNITED STATES TARGETING UNITED STATES PERSONS OUTSIDE THE UNITED STATES

SEC. 703. [50 U.S.C. § 1881b]

(a) JURISDICTION OF THE FOREIGN INTELLIGENCE SURVEILLANCE COURT.—

(1) IN GENERAL.—The Foreign Intelligence Surveillance Court shall have jurisdiction to review an application and to enter an order approving the targeting of a United States person reasonably believed to be located outside the United States to acquire foreign intelligence information, if the acquisition constitutes electronic surveillance or the acquisition of stored electronic communications or stored electronic data that requires an order under this Act, and such acquisition is conducted within the United States.

(2) LIMITATION.—If a United States person targeted under this subsection is reasonably believed to be located in the United States

during the effective period of an order issued pursuant to subsection (c), an acquisition targeting such United States person under this section shall cease unless the targeted United States person is again reasonably believed to be located outside the United States while an order issued pursuant to subsection (c) is in effect. Nothing in this section shall be construed to limit the authority of the Government to seek an order or authorization under, or otherwise engage in any activity that is authorized under, any other title of this Act.

(b) APPLICATION.—

(1) IN GENERAL.—Each application for an order under this section shall be made by a Federal officer in writing upon oath or affirmation to a judge having jurisdiction under subsection (a)(1). Each application shall require the approval of the Attorney General based upon the Attorney General’s finding that it satisfies the criteria and requirements of such application, as set forth in this section, and shall include—

- (A) the identity of the Federal officer making the application;
- (B) the identity, if known, or a description of the United States person who is the target of the acquisition;
- (C) a sworn statement of the facts and circumstances relied upon to justify the applicant’s belief that the United States person who is the target of the acquisition is—
 - (i) a person reasonably believed to be located outside the United States; and
 - (ii) a foreign power, an agent of a foreign power, or an officer or employee of a foreign power;
- (D) a statement of proposed minimization procedures that meet the definition of minimization procedures under section 101(h) or 301(4), as appropriate;
- (E) a description of the nature of the information sought and the type of communications or activities to be subjected to acquisition;
- (F) a certification made by the Attorney General or an official specified in section 104(a)(6) that—
 - (i) the certifying official deems the information sought to be foreign intelligence information;
 - (ii) a significant purpose of the acquisition is to obtain foreign intelligence information;
 - (iii) such information cannot reasonably be obtained by normal investigative techniques;

(iv) designates the type of foreign intelligence information being sought according to the categories described in section 101(e); and
(v) includes a statement of the basis for the certification that—

(I) the information sought is the type of foreign intelligence information designated; and

(II) such information cannot reasonably be obtained by normal investigative techniques;

(G) a summary statement of the means by which the acquisition will be conducted and whether physical entry is required to effect the acquisition;

(H) the identity of any electronic communication service provider necessary to effect the acquisition, provided that the application is not required to identify the specific facilities, places, premises, or property at which the acquisition authorized under this section will be directed or conducted;

(I) a statement of the facts concerning any previous applications that have been made to any judge of the Foreign Intelligence Surveillance Court involving the United States person specified in the application and the action taken on each previous application;

(J) a statement of the period of time for which the acquisition is required to be maintained, provided that such period of time shall not exceed 90 days per application;

(K) a certification by the applicant that, to the best knowledge of the applicant, the Attorney General or a designated attorney for the Government has been apprised of all information that might reasonably—

(i) call into question the accuracy of the application or the reasonableness of any assessment in the application conducted by the department or agency on whose behalf the application is made; or

(ii) otherwise raise doubts with respect to the findings required under subsection (c); and

(L) non-cumulative information known to the applicant or declarant that is potentially exculpatory regarding the requested legal findings or any assessment in the application.

(2) OTHER REQUIREMENTS OF THE ATTORNEY GENERAL.—The Attorney General may require any other affidavit or certification from any other officer in connection with the application.

(3) OTHER REQUIREMENTS OF THE JUDGE.—The judge may require the applicant to furnish such other information as may be necessary to make the findings required by subsection (c)(1).

(c) ORDER.—

(1) FINDINGS.—Upon an application made pursuant to subsection (b), the Foreign Intelligence Surveillance Court shall enter an ex parte order as requested or as modified by the Court approving the acquisition if the Court finds that—

(A) the application has been made by a Federal officer and approved by the Attorney General;

(B) on the basis of the facts submitted by the applicant, for the United States person who is the target of the acquisition, there is probable cause to believe that the target is—

(i) a person reasonably believed to be located outside the United States; and

(ii) a foreign power, an agent of a foreign power, or an officer or employee of a foreign power;

(C) the proposed minimization procedures meet the definition of minimization procedures under section 101(h) or 301(4), as appropriate; and

(D) the application that has been filed contains all statements and certifications required by subsection (b) and the certification or certifications are not clearly erroneous on the basis of the statement made under subsection (b)(1)(F)(v) and any other information furnished under subsection (b)(3).

(2) PROBABLE CAUSE.—In determining whether or not probable cause exists for purposes of paragraph (1)(B), a judge having jurisdiction under subsection (a)(1) may consider past activities of the target and facts and circumstances relating to current or future activities of the target. No United States person may be considered a foreign power, agent of a foreign power, or officer or employee of a foreign power solely upon the basis of activities protected by the first amendment to the Constitution of the United States.

(3) REVIEW.—

(A) LIMITATION ON REVIEW.—Review by a judge having jurisdiction under subsection (a)(1) shall be limited to that required to make the findings described in paragraph (1).

(B) REVIEW OF PROBABLE CAUSE.—If the judge determines that the facts submitted under subsection (b) are insufficient to establish probable cause under paragraph (1)(B), the judge shall enter an order so stating and provide a written statement for the

record of the reasons for the determination. The Government may appeal an order under this subparagraph pursuant to subsection (f).

(C) REVIEW OF MINIMIZATION PROCEDURES.—If the judge determines that the proposed minimization procedures referred to in paragraph (1)(C) do not meet the definition of minimization procedures under section 101(h) or 301(4), as appropriate, the judge shall enter an order so stating and provide a written statement for the record of the reasons for the determination. The Government may appeal an order under this subparagraph pursuant to subsection (f).

(D) REVIEW OF CERTIFICATION.—If the judge determines that an application pursuant to subsection (b) does not contain all of the required elements, or that the certification or certifications are clearly erroneous on the basis of the statement made under subsection (b)(1)(F)(v) and any other information furnished under subsection (b)(3), the judge shall enter an order so stating and provide a written statement for the record of the reasons for the determination. The Government may appeal an order under this subparagraph pursuant to subsection (f).

(4) SPECIFICATIONS.—An order approving an acquisition under this subsection shall specify—

(A) the identity, if known, or a description of the United States person who is the target of the acquisition identified or described in the application pursuant to subsection (b)(1)(B);

(B) if provided in the application pursuant to subsection (b)(1)(H), the nature and location of each of the facilities or places at which the acquisition will be directed;

(C) the nature of the information sought to be acquired and the type of communications or activities to be subjected to acquisition;

(D) a summary of the means by which the acquisition will be conducted and whether physical entry is required to effect the acquisition; and

(E) the period of time during which the acquisition is approved.

(5) DIRECTIVES.—An order approving an acquisition under this subsection shall direct—

(A) that the minimization procedures referred to in paragraph (1)(C), as approved or modified by the Court, be followed;

(B) if applicable, an electronic communication service provider to provide to the Government forthwith all information, facilities,

or assistance necessary to accomplish the acquisition authorized under such order in a manner that will protect the secrecy of the acquisition and produce a minimum of interference with the services that such electronic communication service provider is providing to the target of the acquisition;

(C) if applicable, an electronic communication service provider to maintain under security procedures approved by the Attorney General any records concerning the acquisition or the aid furnished that such electronic communication service provider wishes to maintain; and

(D) if applicable, that the Government compensate, at the prevailing rate, such electronic communication service provider for providing such information, facilities, or assistance.

(6) DURATION.—An order approved under this subsection shall be effective for a period not to exceed 90 days and such order may be renewed for additional 90-day periods upon submission of renewal applications meeting the requirements of subsection (b).

(7) COMPLIANCE.—At or prior to the end of the period of time for which an acquisition is approved by an order or extension under this section, the judge may assess compliance with the minimization procedures referred to in paragraph (1)(C) by reviewing the circumstances under which information concerning United States persons was acquired, retained, or disseminated.

(d) EMERGENCY AUTHORIZATION.—

(1) AUTHORITY FOR EMERGENCY AUTHORIZATION.—Notwithstanding any other provision of this Act, if the Attorney General reasonably determines that—

(A) an emergency situation exists with respect to the acquisition of foreign intelligence information for which an order may be obtained under subsection (c) before an order authorizing such acquisition can with due diligence be obtained, and

(B) the factual basis for issuance of an order under this subsection to approve such acquisition exists,

the Attorney General may authorize such acquisition if a judge having jurisdiction under subsection (a)(1) is informed by the Attorney General, or a designee of the Attorney General, at the time of such authorization that the decision has been made to conduct such acquisition and if an application in accordance with this section is made to a judge of the Foreign Intelligence Surveillance Court as soon as practicable, but not more than 7 days after the Attorney General authorizes such acquisition.

(2) MINIMIZATION PROCEDURES.—If the Attorney General authorizes an acquisition under paragraph (1), the Attorney General shall require that the minimization procedures referred to in subsection (c)(1)(C) for the issuance of a judicial order be followed.

(3) TERMINATION OF EMERGENCY AUTHORIZATION.—In the absence of a judicial order approving an acquisition under paragraph (1), such acquisition shall terminate when the information sought is obtained, when the application for the order is denied, or after the expiration of 7 days from the time of authorization by the Attorney General, whichever is earliest.

(4) USE OF INFORMATION.—If an application for approval submitted pursuant to paragraph (1) is denied, or in any other case where the acquisition is terminated and no order is issued approving the acquisition, no information obtained or evidence derived from such acquisition, except under circumstances in which the target of the acquisition is determined not to be a United States person, shall be received in evidence or otherwise disclosed in any trial, hearing, or other proceeding in or before any court, grand jury, department, office, agency, regulatory body, legislative committee, or other authority of the United States, a State, or political subdivision thereof, and no information concerning any United States person acquired from such acquisition shall subsequently be used or disclosed in any other manner by Federal officers or employees without the consent of such person, except with the approval of the Attorney General if the information indicates a threat of death or serious bodily harm to any person.

(e) RELEASE FROM LIABILITY.—No cause of action shall lie in any court against any electronic communication service provider for providing any information, facilities, or assistance in accordance with an order or request for emergency assistance issued pursuant to subsection (c) or (d), respectively.

(f) APPEAL.—

(1) APPEAL TO THE FOREIGN INTELLIGENCE SURVEILLANCE COURT OF REVIEW.—The Government may file a petition with the Foreign Intelligence Surveillance Court of Review for review of an order issued pursuant to subsection (c). The Court of Review shall have jurisdiction to consider such petition and shall provide a written statement for the record of the reasons for a decision under this paragraph.

(2) CERTIORARI TO THE SUPREME COURT.—The Government may file a petition for a writ of certiorari for review of a decision of the Court of Review issued under paragraph (1). The record for such review shall be transmitted under seal to the Supreme Court of the United States, which shall have jurisdiction to review such decision.

(g) CONSTRUCTION.—Except as provided in this section, nothing in this Act shall be construed to require an application for a court order for an acquisition that is targeted in accordance with this section at a United States person reasonably believed to be located outside the United States.

**OTHER ACQUISITIONS TARGETING UNITED STATES PERSONS
OUTSIDE THE UNITED STATES**

SEC. 704. [50 U.S.C. § 1881c]

(a) JURISDICTION AND SCOPE.—

(1) JURISDICTION.—The Foreign Intelligence Surveillance Court shall have jurisdiction to enter an order pursuant to subsection (c).

(2) SCOPE.—No element of the intelligence community may intentionally target, for the purpose of acquiring foreign intelligence information, a United States person reasonably believed to be located outside the United States under circumstances in which the targeted United States person has a reasonable expectation of privacy and a warrant would be required if the acquisition were conducted inside the United States for law enforcement purposes, unless a judge of the Foreign Intelligence Surveillance Court has entered an order with respect to such targeted United States person or the Attorney General has authorized an emergency acquisition pursuant to subsection (c) or (d), respectively, or any other provision of this Act.

(3) LIMITATIONS.—

(A) MOVING OR MISIDENTIFIED TARGETS.—If a United States person targeted under this subsection is reasonably believed to be located in the United States during the effective period of an order issued pursuant to subsection (c), an acquisition targeting such United States person under this section shall cease unless the targeted United States person is again reasonably believed to be located outside the United States during the effective period of such order.

(B) APPLICABILITY.—If an acquisition for foreign intelligence purposes is to be conducted inside the United States and could be authorized under section 703, the acquisition may only be conducted if authorized under section 703 or in accordance with another provision of this Act other than this section.

(C) CONSTRUCTION.—Nothing in this paragraph shall be construed to limit the authority of the Government to seek an order or authorization under, or otherwise engage in any activity that is authorized under, any other title of this Act.

(b) APPLICATION.—Each application for an order under this section shall be made by a Federal officer in writing upon oath or affirmation to a judge having jurisdiction under subsection (a)(1). Each application shall require the approval of the Attorney General based upon the Attorney General’s finding that it satisfies the criteria and requirements of such application as set forth in this section and shall include—

- (1) the identity of the Federal officer making the application;
- (2) the identity, if known, or a description of the specific United States person who is the target of the acquisition;
- (3) a sworn statement of the facts and circumstances relied upon to justify the applicant’s belief that the United States person who is the target of the acquisition is—
 - (A) a person reasonably believed to be located outside the United States; and
 - (B) a foreign power, an agent of a foreign power, or an officer or employee of a foreign power;
- (4) a statement of proposed minimization procedures that meet the definition of minimization procedures under section 101(h) or 301(4), as appropriate;
- (5) a certification made by the Attorney General, an official specified in section 104(a)(6), or the head of an element of the intelligence community that—
 - (A) the certifying official deems the information sought to be foreign intelligence information; and
 - (B) a significant purpose of the acquisition is to obtain foreign intelligence information;
- (6) a statement of the facts concerning any previous applications that have been made to any judge of the Foreign Intelligence Surveillance Court involving the United States person specified in the application and the action taken on each previous application;
- (7) a statement of the period of time for which the acquisition is required to be maintained, provided that such period of time shall not exceed 90 days per application;
- (8) a certification by the applicant that, to the best knowledge of the applicant, the Attorney General or a designated attorney for the Government has been apprised of all information that might reasonably—
 - (A) call into question the accuracy of the application or the reasonableness of any assessment in the application conducted by the department or agency on whose behalf the application is made; or

(B) otherwise raise doubts with respect to the findings required under subsection (c); and

(9) non-cumulative information known to the applicant or declarant that is potentially exculpatory regarding the requested legal findings or any assessment in the application.

(c) ORDER.—

(1) FINDINGS.—Upon an application made pursuant to subsection (b), the Foreign Intelligence Surveillance Court shall enter an ex parte order as requested or as modified by the Court if the Court finds that—

(A) the application has been made by a Federal officer and approved by the Attorney General;

(B) on the basis of the facts submitted by the applicant, for the United States person who is the target of the acquisition, there is probable cause to believe that the target is—

(i) a person reasonably believed to be located outside the United States; and

(ii) a foreign power, an agent of a foreign power, or an officer or employee of a foreign power;

(C) the proposed minimization procedures, with respect to their dissemination provisions, meet the definition of minimization procedures under section 101(h) or 301(4), as appropriate; and

(D) the application that has been filed contains all statements and certifications required by subsection (b) and the certification provided under subsection (b)(5) is not clearly erroneous on the basis of the information furnished under subsection (b).

(2) PROBABLE CAUSE.—In determining whether or not probable cause exists for purposes of paragraph (1)(B), a judge having jurisdiction under subsection (a)(1) may consider past activities of the target and facts and circumstances relating to current or future activities of the target. No United States person may be considered a foreign power, agent of a foreign power, or officer or employee of a foreign power solely upon the basis of activities protected by the first amendment to the Constitution of the United States.

(3) REVIEW.—

(A) LIMITATIONS ON REVIEW.—Review by a judge having jurisdiction under subsection (a)(1) shall be limited to that required to make the findings described in paragraph (1). The judge shall not have jurisdiction to review the means by which an acquisition under this section may be conducted.

(B) REVIEW OF PROBABLE CAUSE.—If the judge determines that the facts submitted under subsection (b) are insufficient to

establish probable cause to issue an order under this subsection, the judge shall enter an order so stating and provide a written statement for the record of the reasons for such determination. The Government may appeal an order under this subparagraph pursuant to subsection (e).

(C) REVIEW OF MINIMIZATION PROCEDURES.—If the judge determines that the minimization procedures applicable to dissemination of information obtained through an acquisition under this subsection do not meet the definition of minimization procedures under section 101(h) or 301(4), as appropriate, the judge shall enter an order so stating and provide a written statement for the record of the reasons for such determination. The Government may appeal an order under this subparagraph pursuant to subsection (e).

(D) SCOPE OF REVIEW OF CERTIFICATION.—If the judge determines that an application under subsection (b) does not contain all the required elements, or that the certification provided under subsection (b)(5) is clearly erroneous on the basis of the information furnished under subsection (b), the judge shall enter an order so stating and provide a written statement for the record of the reasons for such determination. The Government may appeal an order under this subparagraph pursuant to subsection (e).

(4) DURATION.—An order under this paragraph shall be effective for a period not to exceed 90 days and such order may be renewed for additional 90-day periods upon submission of renewal applications meeting the requirements of subsection (b).

(5) COMPLIANCE.—At or prior to the end of the period of time for which an order or extension is granted under this section, the judge may assess compliance with the minimization procedures referred to in paragraph (1)(C) by reviewing the circumstances under which information concerning United States persons was disseminated, provided that the judge may not inquire into the circumstances relating to the conduct of the acquisition.

(d) EMERGENCY AUTHORIZATION.—

(1) AUTHORITY FOR EMERGENCY AUTHORIZATION.—Notwithstanding any other provision of this section, if the Attorney General reasonably determines that—

(A) an emergency situation exists with respect to the acquisition of foreign intelligence information for which an order may be

obtained under subsection (c) before an order under that subsection can, with due diligence, be obtained, and
(B) the factual basis for the issuance of an order under this section exists,

the Attorney General may authorize the emergency acquisition if a judge having jurisdiction under subsection (a)(1) is informed by the Attorney General or a designee of the Attorney General at the time of such authorization that the decision has been made to conduct such acquisition and if an application in accordance with this section is made to a judge of the Foreign Intelligence Surveillance Court as soon as practicable, but not more than 7 days after the Attorney General authorizes such acquisition.

(2) MINIMIZATION PROCEDURES.—If the Attorney General authorizes an emergency acquisition under paragraph (1), the Attorney General shall require that the minimization procedures referred to in subsection (c)(1)(C) be followed.

(3) TERMINATION OF EMERGENCY AUTHORIZATION.—In the absence of an order under subsection (c), an emergency acquisition under paragraph (1) shall terminate when the information sought is obtained, if the application for the order is denied, or after the expiration of 7 days from the time of authorization by the Attorney General, whichever is earliest.

(4) USE OF INFORMATION.—If an application submitted to the Court pursuant to paragraph (1) is denied, or in any other case where the acquisition is terminated and no order with respect to the target of the acquisition is issued under subsection (c), no information obtained or evidence derived from such acquisition, except under circumstances in which the target of the acquisition is determined not to be a United States person, shall be received in evidence or otherwise disclosed in any trial, hearing, or other proceeding in or before any court, grand jury, department, office, agency, regulatory body, legislative committee, or other authority of the United States, a State, or political subdivision thereof, and no information concerning any United States person acquired from such acquisition shall subsequently be used or disclosed in any other manner by Federal officers or employees without the consent of such person, except with the approval of the Attorney General if the information indicates a threat of death or serious bodily harm to any person.

(e) APPEAL.—

(1) APPEAL TO THE COURT OF REVIEW.—The Government may file a petition with the Foreign Intelligence Surveillance Court of Review for review of an order issued pursuant to subsection (c). The Court of

Review shall have jurisdiction to consider such petition and shall provide a written statement for the record of the reasons for a decision under this paragraph.

(2) CERTIORARI TO THE SUPREME COURT.—The Government may file a petition for a writ of certiorari for review of a decision of the Court of Review issued under paragraph (1). The record for such review shall be transmitted under seal to the Supreme Court of the United States, which shall have jurisdiction to review such decision.

JOINT APPLICATIONS AND CONCURRENT AUTHORIZATIONS

SEC. 705. [50 U.S.C. § 1881d]

(a) JOINT APPLICATIONS AND ORDERS.—If an acquisition targeting a United States person under section 703 or 704 is proposed to be conducted both inside and outside the United States, a judge having jurisdiction under section 703(a)(1) or 704(a)(1) may issue simultaneously, upon the request of the Government in a joint application complying with the requirements of sections 703(b) and 704(b), orders under sections 703(c) and 704(c), as appropriate.

(b) CONCURRENT AUTHORIZATION.—If an order authorizing electronic surveillance or physical search has been obtained under section 105 or 304, the Attorney General may authorize, for the effective period of that order, without an order under section 703 or 704, the targeting of that United States person for the purpose of acquiring foreign intelligence information while such person is reasonably believed to be located outside the United States.

(c) EMERGENCY AUTHORIZATION.—

(1) CONCURRENT AUTHORIZATION.—If the Attorney General authorized the emergency employment of electronic surveillance or a physical search pursuant to section 105 or 304, the Attorney General may authorize, for the effective period of the emergency authorization and subsequent order pursuant to section 105 or 304, without a separate order under section 703 or 704, the targeting of a United States person subject to such emergency employment for the purpose of acquiring foreign intelligence information while such United States person is reasonably believed to be located outside the United States.

(2) USE OF INFORMATION.—If an application submitted to the Court pursuant to section 104 or 303 is denied, or in any other case in which the acquisition pursuant to paragraph (1) is terminated and no order with respect to the target of the acquisition is issued under section 105 or 304, all information obtained or evidence derived from such acquisition shall be handled in accordance with section 704(d)(4).

USE OF INFORMATION ACQUIRED UNDER TITLE VII

SEC. 706. [50 U.S.C. § 1881e]

(a) INFORMATION ACQUIRED UNDER SECTION 702.—

(1) IN GENERAL.—Information acquired from an acquisition conducted under section 702 shall be deemed to be information acquired from an electronic surveillance pursuant to title I for purposes of section 106, except for the purposes of subsection (j) of such section.

(2) UNITED STATES PERSONS.—

(A) IN GENERAL.—Any information concerning a United States person acquired under section 702 shall not be used in evidence against that United States person pursuant to paragraph (1) in any criminal proceeding unless—

(i) the Federal Bureau of Investigation obtained an order of the Foreign Intelligence Surveillance Court to access such information pursuant to section 702(f)(2); or

(ii) the Attorney General determines that—

(I) the criminal proceeding affects, involves, or is related to the national security of the United States; or

(II) the criminal proceeding involves—

(aa) death;

(bb) kidnapping;

(cc) serious bodily injury, as defined in section 1365 of title 18, United States Code;

(dd) conduct that constitutes a criminal offense that is a specified offense against a minor, as defined in section 111 of the Adam Walsh Child Protection and Safety Act of 2006 (34 U.S.C. 20911);

(ee) incapacitation or destruction of critical infrastructure, as defined in section 1016(e) of the USA PATRIOT Act (42 U.S.C. 5195c(e));

(ff) cybersecurity, including conduct described in section 1016(e) of the USA PATRIOT Act (42 U.S.C. 5195c(e)) or section 1029, 1030, or 2511 of title 18, United States Code;

(gg) transnational crime, including transnational narcotics trafficking and transnational organized crime; or
(hh) human trafficking.

(B) NO JUDICIAL REVIEW.—A determination by the Attorney General under subparagraph (A)(ii) is not subject to judicial review.

(b) INFORMATION ACQUIRED UNDER SECTION 703.—Information acquired from an acquisition conducted under section 703 shall be deemed to be information acquired from an electronic surveillance pursuant to title I for purposes of section 106.

CONGRESSIONAL OVERSIGHT

SEC. 707. [50 U.S.C. § 1881f]

(a) SEMIANNUAL REPORT.—Not less frequently than once every 6 months, the Attorney General shall fully inform, in a manner consistent with national security, the congressional intelligence committees and the Committees on the Judiciary of the Senate and the House of Representatives, consistent with the Rules of the House of Representatives, the Standing Rules of the Senate, and Senate Resolution 400 of the 94th Congress or any successor Senate resolution, concerning the implementation of this title.

(b) CONTENT.—Each report under subsection (a) shall include—

(1) with respect to section 702—

(A) any certifications submitted in accordance with section 702(h) during the reporting period;

(B) with respect to each determination under section 702(c)(2), the reasons for exercising the authority under such section;

(C) any directives issued under section 702(i) during the reporting period;

(D) a description of the judicial review during the reporting period of such certifications and targeting and minimization procedures adopted in accordance with subsections (d) and (e) of section 702 and utilized with respect to an acquisition under such section, including a copy of an order or pleading in connection with such review that contains a significant legal interpretation of the provisions of section 702;

(E) any actions taken to challenge or enforce a directive under paragraph (4) or (5) of section 702(i);

- (F) any compliance reviews conducted by the Attorney General or the Director of National Intelligence of acquisitions authorized under section 702(a);
 - (G) a description of any incidents of noncompliance—
 - (i) with a directive issued by the Attorney General and the Director of National Intelligence under section 702(i), including incidents of noncompliance by a specified person to whom the Attorney General and Director of National Intelligence issued a directive under section 702(i); and
 - (ii) by an element of the intelligence community with procedures and guidelines adopted in accordance with subsections (d), (e), (f)(1), and (g) of section 702; and
 - (H) any procedures implementing section 702;
- (2) with respect to section 703—
- (A) the total number of applications made for orders under section 703(b);
 - (B) the total number of such orders—
 - (i) granted;
 - (ii) modified; and
 - (iii) denied; and
 - (C) the total number of emergency acquisitions authorized by the Attorney General under section 703(d) and the total number of subsequent orders approving or denying such acquisitions; and
- (3) with respect to section 704—
- (A) the total number of applications made for orders under section 704(b);
 - (B) the total number of such orders—
 - (i) granted;
 - (ii) modified; and
 - (iii) denied; and
 - (C) the total number of emergency acquisitions authorized by the Attorney General under section 704(d) and the total number of subsequent orders approving or denying such applications.

SAVINGS PROVISION

SEC. 708. [50 U.S.C. § 1881g]

Nothing in this title shall be construed to limit the authority of the Government to seek an order or authorization under, or otherwise engage in any activity that is authorized under, any other title of this Act.

PENALTIES FOR UNAUTHORIZED DISCLOSURE

SEC. 709. [18 U.S.C. § 1623]

(a) **OFFENSE.**—A person is guilty of an offense under this section if that person knowingly and willfully communicates, furnishes, transmits, or otherwise makes available to an unauthorized person, or publishes, or uses in any manner prejudicial to the safety or interest of the United States or for the benefit of any foreign government to the detriment of the United States any classified information that contains the contents of any communication acquired under this title to which a known United States person is a party.

(b) **PENALTY.**—A person guilty of an offense in this section shall be fined under title 18, imprisoned for not more than 8 years, or both.

(c) **JURISDICTION.**—There is Federal jurisdiction over an offense under this section if the person committing the offense was an officer or employee of the United States at the time the offense was committed.

**TITLE VIII—PROTECTION OF PERSONS ASSISTING
THE GOVERNMENT**

DEFINITIONS

SEC. 801. [50 U.S.C. § 1885]

In this title:

(1) **ASSISTANCE.**—The term “assistance” means the provision of, or the provision of access to, information (including communication contents, communications records, or other information relating to a customer or communication), facilities, or another form of assistance.

(2) **CIVIL ACTION.**—The term “civil action” includes a covered civil action.

(3) **CONGRESSIONAL INTELLIGENCE COMMITTEES.**—The term “congressional intelligence committees” means—

(A) the Select Committee on Intelligence of the Senate; and

(B) the Permanent Select Committee on Intelligence of the House of Representatives.

(4) **CONTENTS.**—The term “contents” has the meaning given that term in section 101(n).

(5) **COVERED CIVIL ACTION.**—The term “covered civil action” means a civil action filed in a Federal or State court that—

(A) alleges that an electronic communication service provider furnished assistance to an element of the intelligence community; and

(B) seeks monetary or other relief from the electronic communication service provider related to the provision of such assistance.

(6) ELECTRONIC COMMUNICATION SERVICE PROVIDER.—The term “electronic communication service provider” means—

- (A) a telecommunications carrier, as that term is defined in section 3 of the Communications Act of 1934 (47 U.S.C. 153);
- (B) a provider of electronic communication service, as that term is defined in section 2510 of title 18, United States Code;
- (C) a provider of a remote computing service, as that term is defined in section 2711 of title 18, United States Code;
- (D) any other communication service provider who has access to wire or electronic communications either as such communications are transmitted or as such communications are stored;
- (E) any other service provider who has access to equipment that is being or may be used to transmit or store wire or electronic communications, but not including any entity that serves primarily as—
 - (i) a public accommodation facility, as that term is defined in section 501(4);
 - (ii) a dwelling, as that term is defined in section 802 of the Fair Housing Act (42 U.S.C. 3602);
 - (iii) a community facility, as that term is defined in section 315 of the Defense Housing and Community Facilities and Services Act of 1951 (42 U.S.C. 1592n); or
 - (iv) a food service establishment, as that term is defined in section 281 of the Agricultural Marketing Act of 1946 (7 U.S.C. 1638);
- (F) a parent, subsidiary, affiliate, successor, or assignee of an entity described in subparagraph (A), (B), (C), or (D);
- (G) an officer, employee, custodian, or agent of an entity described in subparagraph (A), (B), (C), (D), (E), or (F).

(7) INTELLIGENCE COMMUNITY.—The term “intelligence community” has the meaning given the term in section 3(4) of the National Security Act of 1947 (50 U.S.C. 3003(4)).

(8) PERSON.—The term “person” means—

- (A) an electronic communication service provider; or
- (B) a landlord, custodian, or other person who may be authorized or required to furnish assistance pursuant to—
 - (i) an order of the court established under section 103(a) directing such assistance;
 - (ii) a certification in writing under section 2511(2)(a)(ii)(B) or 2709(b) of title 18, United States Code; or

(iii) a directive under section 102(a)(4), 105B(e), as added by section 2 of the Protect America Act of 2007 (Public Law 110-55), or 702(i).

(9) STATE.—The term “State” means any State, political subdivision of a State, the Commonwealth of Puerto Rico, the District of Columbia, and any territory or possession of the United States, and includes any officer, public utility commission, or other body authorized to regulate an electronic communication service provider.

PROCEDURES FOR IMPLEMENTING STATUTORY DEFENSES

SEC. 802. [50 U.S.C. § 1885a]

(a) REQUIREMENT FOR CERTIFICATION.—Notwithstanding any other provision of law, a civil action may not lie or be maintained in a Federal or State court against any person for providing assistance to an element of the intelligence community, and shall be promptly dismissed, if the Attorney General certifies to the district court of the United States in which such action is pending that—

(1) any assistance by that person was provided pursuant to an order of the court established under section 103(a) directing such assistance;

(2) any assistance by that person was provided pursuant to a certification in writing under section 2511(2)(a)(ii)(B) or 2709(b) of title 18, United States Code;

(3) any assistance by that person was provided pursuant to a directive under section 102(a)(4), 105B(e) as added by section 2 of the Protect America Act of 2007 (Public Law 110-55), or 702(i) directing such assistance;

(4) in the case of a covered civil action, the assistance alleged to have been provided by the electronic communication service provider was—

(A) in connection with an intelligence activity involving communications that was—

(i) authorized by the President during the period beginning on September 11, 2001, and ending on January 17, 2007; and

(ii) designed to detect or prevent a terrorist attack, or activities in preparation for a terrorist attack, against the United States; and

(B) the subject of a written request or directive, or a series of written requests or directives, from the Attorney General or the head of an element of the intelligence community (or the deputy of such person) to the electronic communication service provider indicating that the activity was—

- (i) authorized by the President; and
- (ii) determined to be lawful; or

(5) the person did not provide the alleged assistance.

(b) JUDICIAL REVIEW.—

(1) REVIEW OF CERTIFICATIONS.—A certification under subsection (a) shall be given effect unless the court finds that such certification is not supported by substantial evidence provided to the court pursuant to this section.

(2) SUPPLEMENTAL MATERIALS.—In its review of a certification under subsection (a), the court may examine the court order, certification, written request, or directive described in subsection (a) and any relevant court order, certification, written request, or directive submitted pursuant to subsection (d).

(c) LIMITATIONS ON DISCLOSURE.—If the Attorney General files a declaration under section 1746 of title 28, United States Code, that disclosure of a certification made pursuant to subsection (a) or the supplemental materials provided pursuant to subsection (b) or (d) would harm the national security of the United States, the court shall—

(1) review such certification and the supplemental materials in camera and ex parte; and

(2) limit any public disclosure concerning such certification and the supplemental materials, including any public order following such in camera and ex parte review, to a statement as to whether the case is dismissed and a description of the legal standards that govern the order, without disclosing the paragraph of subsection (a) that is the basis for the certification.

(d) ROLE OF THE PARTIES.—Any plaintiff or defendant in a civil action may submit any relevant court order, certification, written request, or directive to the district court referred to in subsection (a) for review and shall be permitted to participate in the briefing or argument of any legal issue in a judicial proceeding conducted pursuant to this section, but only to the extent that such participation does not require the disclosure of classified information to such party. To the extent that classified information is relevant to the proceeding or would be revealed in the determination of an issue, the court shall review such information in camera and ex parte, and shall issue any part of the court's written order that would reveal classified information in camera and ex parte and maintain such part under seal.

(e) NONDELEGATION.—The authority and duties of the Attorney General under this section shall be performed by the Attorney General (or Acting Attorney General) or the Deputy Attorney General.

- (f) **APPEAL.**—The courts of appeals shall have jurisdiction of appeals from interlocutory orders of the district courts of the United States granting or denying a motion to dismiss or for summary judgment under this section.
- (g) **REMOVAL.**—A civil action against a person for providing assistance to an element of the intelligence community that is brought in a State court shall be deemed to arise under the Constitution and laws of the United States and shall be removable under section 1441 of title 28, United States Code.
- (h) **RELATIONSHIP TO OTHER LAWS.**—Nothing in this section shall be construed to limit any otherwise available immunity, privilege, or defense under any other provision of law.
- (i) **APPLICABILITY.**—This section shall apply to a civil action pending on or filed after the date of the enactment of the FISA Amendments Act of 2008.

PREEMPTION

SEC. 803. [50 U.S.C. § 1885b]

- (a) **IN GENERAL.**—No State shall have authority to—
- (1) conduct an investigation into an electronic communication service provider’s alleged assistance to an element of the intelligence community;
 - (2) require through regulation or any other means the disclosure of information about an electronic communication service provider’s alleged assistance to an element of the intelligence community;
 - (3) impose any administrative sanction on an electronic communication service provider for assistance to an element of the intelligence community; or
 - (4) commence or maintain a civil action or other proceeding to enforce a requirement that an electronic communication service provider disclose information concerning alleged assistance to an element of the intelligence community.
- (b) **SUITS BY THE UNITED STATES.**—The United States may bring suit to enforce the provisions of this section.
- (c) **JURISDICTION.**—The district courts of the United States shall have jurisdiction over any civil action brought by the United States to enforce the provisions of this section.
- (d) **APPLICATION.**—This section shall apply to any investigation, action, or proceeding that is pending on or commenced after the date of the enactment of the FISA Amendments Act of 2008.

REPORTING

SEC. 804. [50 U.S.C. § 1885c]

(a) SEMIANNUAL REPORT.—Not less frequently than once every 6 months, the Attorney General shall, in a manner consistent with national security, the Rules of the House of Representatives, the Standing Rules of the Senate, and Senate Resolution 400 of the 94th Congress or any successor Senate resolution, fully inform the congressional intelligence committees, the Committee on the Judiciary of the Senate, and the Committee on the Judiciary of the House of Representatives concerning the implementation of this title.

(b) CONTENT.—Each report made under subsection (a) shall include—

- (1) any certifications made under section 802;
- (2) a description of the judicial review of the certifications made under section 802; and
- (3) any actions taken to enforce the provisions of section 803.

**SELECTED ADDITIONAL PROVISIONS OF THE
FISA AMENDMENTS ACT OF 2008**

REVIEW OF PREVIOUS ACTIONS

SEC. 301.

(a) DEFINITIONS.—In this section:

(1) APPROPRIATE COMMITTEES OF CONGRESS.—The term “appropriate committees of Congress” means—

- (A) the Select Committee on Intelligence and the Committee on the Judiciary of the Senate; and
- (B) the Permanent Select Committee on Intelligence and the Committee on the Judiciary of the House of Representatives.

(2) FOREIGN INTELLIGENCE SURVEILLANCE COURT.—The term “Foreign Intelligence Surveillance Court” means the court established under section 103(a) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1803(a)).

(3) PRESIDENT’S SURVEILLANCE PROGRAM AND PROGRAM.—The terms “President’s Surveillance Program” and “Program” mean the intelligence activity involving communications that was authorized by the President during the period beginning on September 11, 2001, and ending on January 17, 2007, including the program referred to by the President in a radio address on December 17, 2005 (commonly known as the Terrorist Surveillance Program).

(b) REVIEWS.—

(1) REQUIREMENT TO CONDUCT.—The Inspectors General of the Department of Justice, the Office of the Director of National Intelligence, the National Security Agency, the Department of Defense, and any other element of the intelligence community that participated in the President’s Surveillance Program, shall complete a comprehensive review of, with respect to the oversight authority and responsibility of each such Inspector General—

- (A) all of the facts necessary to describe the establishment, implementation, product, and use of the product of the Program;
- (B) access to legal reviews of the Program and access to information about the Program;
- (C) communications with, and participation of, individuals and entities in the private sector related to the Program;
- (D) interaction with the Foreign Intelligence Surveillance Court and transition to court orders related to the Program; and
- (E) any other matters identified by any such Inspector General that would enable that Inspector General to complete a review of the Program, with respect to such Department or element.

(2) COOPERATION AND COORDINATION.—

(A) COOPERATION.—Each Inspector General required to conduct a review under paragraph (1) shall—

- (i) work in conjunction, to the extent practicable, with any other Inspector General required to conduct such a review; and
- (ii) utilize, to the extent practicable, and not unnecessarily duplicate or delay, such reviews or audits that have been completed or are being undertaken by any such Inspector General or by any other office of the Executive Branch related to the Program.

(B) INTEGRATION OF OTHER REVIEWS.—The Counsel of the Office of Professional Responsibility of the Department of Justice shall provide the report of any investigation conducted by such Office on matters relating to the Program, including any investigation of the process through which legal reviews of the Program were conducted and the substance of such reviews, to the Inspector General of the Department of Justice, who shall integrate the factual findings and conclusions of such investigation into its review.

(C) COORDINATION.—The Inspectors General shall designate one of the Inspectors General required to conduct a review under paragraph (1) that is appointed by the President, by and with the

advice and consent of the Senate, to coordinate the conduct of the reviews and the preparation of the reports.

(c) REPORTS.—

(1) PRELIMINARY REPORTS.—Not later than 60 days after the date of the enactment of this Act, the Inspectors General of the Department of Justice, the Office of the Director of National Intelligence, the National Security Agency, the Department of Defense, and any other Inspector General required to conduct a review under subsection (b)(1), shall submit to the appropriate committees of Congress an interim report that describes the planned scope of such review.

(2) FINAL REPORT.—Not later than 1 year after the date of the enactment of this Act, the Inspectors General of the Department of Justice, the Office of the Director of National Intelligence, the National Security Agency, the Department of Defense, and any other Inspector General required to conduct a review under subsection (b)(1), shall submit to the appropriate committees of Congress, in a manner consistent with national security, a comprehensive report on such reviews that includes any recommendations of any such Inspectors General within the oversight authority and responsibility of any such Inspector General with respect to the reviews.

(3) FORM.—A report under this subsection shall be submitted in unclassified form, but may include a classified annex. The unclassified report shall not disclose the name or identity of any individual or entity of the private sector that participated in the Program or with whom there was communication about the Program, to the extent that information is classified.

(d) RESOURCES.—

(1) EXPEDITED SECURITY CLEARANCE.—The Director of National Intelligence shall ensure that the process for the investigation and adjudication of an application by an Inspector General or any appropriate staff of an Inspector General for a security clearance necessary for the conduct of the review under subsection (b)(1) is carried out as expeditiously as possible.

(2) ADDITIONAL PERSONNEL FOR THE INSPECTORS GENERAL.—An Inspector General required to conduct a review under subsection (b)(1) and submit a report under subsection (c) is authorized to hire such additional personnel as may be necessary to carry out such review and prepare such report in a prompt and timely manner. Personnel authorized to be hired under this paragraph—

(A) shall perform such duties relating to such a review as the relevant Inspector General shall direct; and

(B) are in addition to any other personnel authorized by law.

(3) TRANSFER OF PERSONNEL.—The Attorney General, the Secretary of Defense, the Director of National Intelligence, the Director of the National Security Agency, or the head of any other element of the intelligence community may transfer personnel to the relevant Office of the Inspector General required to conduct a review under subsection (b)(1) and submit a report under subsection (c) and, in addition to any other personnel authorized by law, are authorized to fill any vacancy caused by such a transfer. Personnel transferred under this paragraph shall perform such duties relating to such review as the relevant Inspector General shall direct.

SEVERABILITY

SEC. 401 [50 U.S.C. § 1801 note]

If any provision of this Act, any amendment made by this Act, or the application thereof to any person or circumstances is held invalid, the validity of the remainder of the Act, of any such amendments, and of the application of such provisions to other persons and circumstances shall not be affected thereby.

TRANSITION PROCEDURES

SEC. 404.

(a) TRANSITION PROCEDURES FOR PROTECT AMERICA ACT OF 2007 PROVISIONS.—

(1) CONTINUED EFFECT OF ORDERS, AUTHORIZATIONS, DIRECTIVES.—Except as provided in paragraph (7), notwithstanding any other provision of law, any order, authorization, or directive issued or made pursuant to section 105B of the Foreign Intelligence Surveillance Act of 1978, as added by section 2 of the Protect America Act of 2007 (Public Law 110-55; 121 Stat. 552), shall continue in effect until the expiration of such order, authorization, or directive.

(2) APPLICABILITY OF PROTECT AMERICA ACT OF 2007 TO CONTINUED ORDERS, AUTHORIZATIONS, DIRECTIVES.—Notwithstanding any other provision of this Act, any amendment made by this Act, or the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.)—

(A) subject to paragraph (3), section 105A of such Act, as added by section 2 of the Protect America Act of 2007 (Public Law 110-55; 121 Stat. 552), shall continue to apply to any acquisition conducted pursuant to an order, authorization, or directive referred to in paragraph (1); and

(B) sections 105B and 105C of the Foreign Intelligence Surveillance Act of 1978, as added by sections 2 and 3, respectively, of the Protect America Act of 2007, shall continue to apply with respect to an order, authorization, or directive referred to in paragraph (1) until the later of—

- (i) the expiration of such order, authorization, or directive; or
- (ii) the date on which final judgment is entered for any petition or other litigation relating to such order, authorization, or directive.

(3) USE OF INFORMATION.—Information acquired from an acquisition conducted pursuant to an order, authorization, or directive referred to in paragraph (1) shall be deemed to be information acquired from an electronic surveillance pursuant to title I of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) for purposes of section 106 of such Act (50 U.S.C. 1806), except for purposes of subsection (j) of such section.

(4) PROTECTION FROM LIABILITY.—Subsection (l) of section 105B of the Foreign Intelligence Surveillance Act of 1978, as added by section 2 of the Protect America Act of 2007, shall continue to apply with respect to any directives issued pursuant to such section 105B.

(5) JURISDICTION OF FOREIGN INTELLIGENCE SURVEILLANCE COURT.—Notwithstanding any other provision of this Act or of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.), section 103(e) of the Foreign Intelligence Surveillance Act (50 U.S.C. 1803(e)), as amended by section 5(a) of the Protect America Act of 2007 (Public Law 110-55; 121 Stat. 556), shall continue to apply with respect to a directive issued pursuant to section 105B of the Foreign Intelligence Surveillance Act of 1978, as added by section 2 of the Protect America Act of 2007, until the later of—

- (A) the expiration of all orders, authorizations, or directives referred to in paragraph (1); or
- (B) the date on which final judgment is entered for any petition or other litigation relating to such order, authorization, or directive.

(6) REPORTING REQUIREMENTS.—

(A) CONTINUED APPLICABILITY.—Notwithstanding any other provision of this Act, any amendment made by this Act, the Protect America Act of 2007 (Public Law 110-55), or the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.), section 4 of the Protect America Act of 2007 shall continue

to apply until the date that the certification described in subparagraph (B) is submitted.

(B) CERTIFICATION.—The certification described in this subparagraph is a certification—

- (i) made by the Attorney General;
- (ii) submitted as part of a semi-annual report required by section 4 of the Protect America Act of 2007;
- (iii) that states that there will be no further acquisitions carried out under section 105B of the Foreign Intelligence Surveillance Act of 1978, as added by section 2 of the Protect America Act of 2007, after the date of such certification; and
- (iv) that states that the information required to be included under such section 4 relating to any acquisition conducted under such section 105B has been included in a semi-annual report required by such section 4.

(7) REPLACEMENT OF ORDERS, AUTHORIZATIONS, AND DIRECTIVES.—

(A) IN GENERAL.—If the Attorney General and the Director of National Intelligence seek to replace an authorization issued pursuant to section 105B of the Foreign Intelligence Surveillance Act of 1978, as added by section 2 of the Protect America Act of 2007 (Public Law 110-55), with an authorization under section 702 of the Foreign Intelligence Surveillance Act of 1978 (as added by section 101(a) of this Act), the Attorney General and the Director of National Intelligence shall, to the extent practicable, submit to the Foreign Intelligence Surveillance Court (as such term is defined in section 701(b)(2) of such Act (as so added)) a certification prepared in accordance with subsection (g) of such section 702 and the procedures adopted in accordance with subsections (d) and (e) of such section 702 at least 30 days before the expiration of such authorization.

(B) CONTINUATION OF EXISTING ORDERS.—If the Attorney General and the Director of National Intelligence seek to replace an authorization made pursuant to section 105B of the Foreign Intelligence Surveillance Act of 1978, as added by section 2 of the Protect America Act of 2007 (Public Law 110-55; 121 Stat. 522), by filing a certification in accordance with subparagraph (A), that authorization, and any directives issued thereunder and any order related thereto, shall remain in effect, notwithstanding the expiration provided for in subsection (a) of such section 105B, until the Foreign Intelligence Surveillance Court (as such

term is defined in section 701(b)(2) of the Foreign Intelligence Surveillance Act of 1978 (as so added)) issues an order with respect to that certification under section 702(i)(3) of such Act (as so added) at which time the provisions of that section and of section 702(i)(4) of such Act (as so added) shall apply.

(8) EFFECTIVE DATE.—Paragraphs (1) through (7) shall take effect as if enacted on August 5, 2007.

(b) TRANSITION PROCEDURES FOR FISA AMENDMENTS ACT OF 2008 PROVISIONS.—

(1) ORDERS IN EFFECT ON DECEMBER 31, 2012.—Notwithstanding any other provision of this Act, any amendment made by this Act, or the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.), any order, authorization, or directive issued or made under title VII of the Foreign Intelligence Surveillance Act of 1978, as amended by section 101(a), shall continue in effect until the date of the expiration of such order, authorization, or directive.

(2) APPLICABILITY OF TITLE VII OF FISA TO CONTINUED ORDERS, AUTHORIZATIONS, DIRECTIVES.—Notwithstanding any other provision of this Act, any amendment made by this Act, or the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.), with respect to any order, authorization, or directive referred to in paragraph (1), title VII of such Act, as amended by section 101(a), shall continue to apply until the later of—

- (A) the expiration of such order, authorization, or directive; or
- (B) the date on which final judgment is entered for any petition or other litigation relating to such order, authorization, or directive.

(3) CHALLENGE OF DIRECTIVES; PROTECTION FROM LIABILITY; USE OF INFORMATION.—Notwithstanding any other provision of this Act or of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.)—

- (A) section 103(e) of such Act, as amended by section 403(a)(1)(B)(ii), shall continue to apply with respect to any directive issued pursuant to section 702(h) of such Act, as added by section 101(a);
- (B) section 702(h)(3) of such Act (as so added) shall continue to apply with respect to any directive issued pursuant to section 702(h) of such Act (as so added);
- (C) section 703(e) of such Act (as so added) shall continue to apply with respect to an order or request for emergency assistance under that section;

(D) section 706 of such Act (as so added) shall continue to apply to an acquisition conducted under section 702 or 703 of such Act (as so added); and

(E) section 2511(2)(a)(ii)(A) of title 18, United States Code, as amended by section 101(c)(1), shall continue to apply to an order issued pursuant to section 704 of the Foreign Intelligence Surveillance Act of 1978, as added by section 101(a).

(4) REPORTING REQUIREMENTS.—

(A) CONTINUED APPLICABILITY.—Notwithstanding any other provision of this Act or of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.), section 601(a) of such Act (50 U.S.C. 1871(a)), as amended by section 101(c)(2), and sections 702(l) and 707 of such Act, as added by section 101(a), shall continue to apply until the date that the certification described in subparagraph (B) is submitted.

(B) CERTIFICATION.—The certification described in this subparagraph is a certification—

(i) made by the Attorney General;

(ii) submitted to the Select Committee on Intelligence of the Senate, the Permanent Select Committee on Intelligence of the House of Representatives, and the Committees on the Judiciary of the Senate and the House of Representatives;

(iii) that states that there will be no further acquisitions carried out under title VII of the Foreign Intelligence Surveillance Act of 1978, as amended by section 101(a), after the date of such certification; and

(iv) that states that the information required to be included in a review, assessment, or report under section 601 of such Act, as amended by section 101(c), or section 702(l) or 707 of such Act, as added by section 101(a), relating to any acquisition conducted under title VII of such Act, as amended by section 101(a), has been included in a review, assessment, or report under such section 601, 702(l), or 707.

(5) TRANSITION PROCEDURES CONCERNING THE TARGETING OF UNITED STATES PERSONS OVERSEAS.—Any authorization in effect on the date of enactment of this Act under section 2.5 of Executive Order 12333 to intentionally target a United States person reasonably believed to be located outside the United States shall continue in effect, and shall constitute a sufficient basis for conducting such an acquisition targeting

a United States person located outside the United States until the earlier of—

(A) the date that authorization expires; or

(B) the date that is 90 days after the date of the enactment of this Act.

SELECTED ADDITIONAL SAVINGS PROVISIONS

LONE WOLF SAVINGS PROVISION

Pub. L. 108-458, 118 Stat. 3638, § 6001(b) [50 U.S.C. § 1801 note]

(b) SUNSET.—The amendment made by subsection (a) shall be subject to the sunset provision in section 224 of Public Law 107-56 (115 Stat. 295), including the exception provided in subsection (b) of such section 224.

Pub. L. 107-56, 115 Stat. 227, 295 § 22

(a) IN GENERAL.—Except as provided in subsection (b), this title and the amendments made by this title (other than sections 203(a), 203(c), 205, 208, 210, 211, 213, 216, 219, 221, and 222, and the amendments made by those sections) shall cease to have effect on December 31, 2005.

(b) EXCEPTION.—With respect to any particular foreign intelligence investigation that began before the date on which the provisions referred to in subsection (a) cease to have effect, or with respect to any particular offense or potential offense that began or occurred before the date on which such provisions cease to have effect, such provisions shall continue in effect.

Pub. L. 116-69, 133 Stat. 1134, 1143, § 1703(b) [50 U.S.C. § 1801 note]

(b) Section 6001(b)(1) of the Intelligence Reform and Terrorism Prevention Act of 2004 (50 U.S.C. 1801 note) is amended by striking “December 15, 2019” and inserting “March 15, 2020”.

EXPIRED LONE WOLF STATUTORY PROVISION

50 U.S.C. § 1801(b)(1)(C)

(C) engages in international terrorism or activities in preparation therefore [*sic*];

ROVING WIRETAP SAVINGS PROVISION

Pub. L. 109-177, 120 Stat. 192, 195

(b) SECTIONS 206 AND 215 SUNSET.—

FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978

(1) IN GENERAL.—Effective December 31, 2009, the Foreign Intelligence Surveillance Act of 1978 is amended so that sections 501, 502, and 105(c)(2) read as they read on October 25, 2001.

(2) EXCEPTION.—With respect to any particular foreign intelligence investigation that began before the date on which the provisions referred to in paragraph (1) cease to have effect, or with respect to any particular offense or potential offense that began or occurred before the date on which such provisions cease to have effect, such provisions shall continue in effect.

Pub. L. 116-69, 133 Stat. 1134, 1143, § 1703(a)

(a) Section 102(b)(1) of the USA PATRIOT Improvement and Reauthorization Act of 2005 (50 U.S.C. 1805 note) is amended by striking “December 15, 2019” and inserting “March 15, 2020”.

EXPIRED ROVING WIRETAP STATUTORY PROVISION

50 U.S.C. § 1805(c)(2)(B)

(B) that, upon the request of the applicant, a specified communication or other common carrier, landlord, custodian, or other specified person, or in circumstances where the Court finds, based upon specific facts provided in the application, that the actions of the target of the application may have the effect of thwarting the identification of a specified person, such other persons, furnish the applicant forthwith all information, facilities, or technical assistance necessary to accomplish the electronic surveillance in such a manner as will protect its secrecy and produce a minimum of interference with the services that such carrier, landlord, custodian, or other person is providing that target of electronic surveillance;

BUSINESS RECORDS SAVINGS PROVISION

Pub. L. 109-177, 120 Stat. 192, 195

(b) SECTIONS 206 AND 215 SUNSET.—

(1) IN GENERAL.—Effective December 31, 2009, the Foreign Intelligence Surveillance Act of 1978 is amended so that sections 501, 502, and 105(c)(2) read as they read on October 25, 2001.

(2) EXCEPTION.—With respect to any particular foreign intelligence investigation that began before the date on which the provisions referred to in paragraph (1) cease to have effect, or with respect to any particular offense or potential offense that began or occurred before the date on which such provisions cease to have effect, such provisions shall continue in effect.

Pub. L. 116-69, 133 Stat. 1134, 1143, § 1703(a)

(a) Section 102(b)(1) of the USA PATRIOT Improvement and Reauthorization Act of 2005 (50 U.S.C. 1805 note) is amended by striking “December 15, 2019” and inserting “March 15, 2020”.

EXPIRED BUSINESS RECORDS STATUTORY PROVISIONS

ACCESS TO CERTAIN BUSINESS RECORDS FOR FOREIGN INTELLIGENCE AND INTERNATIONAL TERRORISM INVESTIGATIONS

SEC. 501. [50 U.S.C. § 1861]

(a)(1) Subject to paragraph (3), the Director of the Federal Bureau of Investigation or a designee of the Director (whose rank shall be no lower than Assistant Special Agent in Charge) may make an application for an order requiring the production of any tangible things (including books, records, papers, documents, and other items) for an investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution.

(2) An investigation conducted under this section shall

- (A) be conducted under guidelines approved by the Attorney General under Executive Order 12333 (or a successor order); and
- (B) not be conducted of a United States person solely upon the basis of activities protected by the first amendment to the Constitution of the United States.

(3) In the case of an application for an order requiring the production of library circulation records, library patron lists, book sales records, book customer lists, firearms sales records, tax return records, educational records, or medical records containing information that would identify a person, the Director of the Federal Bureau of Investigation may delegate the authority to make such application to either the Deputy Director of the Federal Bureau of Investigation or the Executive Assistant Director for National Security (or any successor position). The Deputy Director or the Executive Assistant Director may not further delegate such authority.

(b) Each application under this section—

(1) shall be made to—

- (A) a judge of the court established by section 103(a); or
- (B) a United States Magistrate Judge under chapter 43 of Title 28, United States Code, who is publicly designated by the Chief Justice of the United States to have the power to hear

- applications and grant orders for the production of tangible things under this section on behalf of a judge of that court; and (2) shall include—
- (A) a specific selection term to be used as the basis for the production of the tangible things sought;
 - (B) in the case of an application other than an application described in subparagraph (C) (including an application for the production of call detail records other than in the manner described in subparagraph (C)), a statement of facts showing that there are reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation (other than a threat assessment) conducted in accordance with subsection (a)(2) to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities, such things being presumptively relevant to an authorized investigation if the applicant shows in the statement of the facts that they pertain to—
 - (i) a foreign power or an agent of a foreign power;
 - (ii) the activities of a suspected agent of a foreign power who is the subject of such authorized investigation; or
 - (iii) an individual in contact with, or known to, a suspected agent of a foreign power who is the subject of such authorized investigation;
 - (C) in the case of an application for the production on an ongoing basis of call detail records created before, on, or after the date of the application relating to an authorized investigation (other than a threat assessment) conducted in accordance with subsection (a)(2) to protect against international terrorism, a statement of facts showing that—
 - (i) there are reasonable grounds to believe that the call detail records sought to be produced based on the specific selection term required under subparagraph (A) are relevant to such investigation; and
 - (ii) there is a reasonable, articulable suspicion that such specific selection term is associated with a foreign power engaged in international terrorism or activities in preparation therefor, or an agent of a foreign power engaged in international terrorism or activities in preparation therefor; and

(D) an enumeration of the minimization procedures adopted by the Attorney General under subsection (g) that are applicable to the retention and dissemination by the Federal Bureau of Investigation of any tangible things to be made available to the Federal Bureau of Investigation based on the order requested in such application.

(c)(1) Upon an application made pursuant to this section, if the judge finds that the application meets the requirements of subsections (a) and (b) and that the minimization procedures submitted in accordance with subsection (b)(2)(D) meet the definition of minimization procedures under subsection (g), the judge shall enter an ex parte order as requested, or as modified, approving the release of tangible things. Such order shall direct that minimization procedures adopted pursuant to subsection (g) be followed.

(2) An order under this subsection—

(A) shall describe the tangible things that are ordered to be produced with sufficient particularity to permit them to be fairly identified, including each specific selection term to be used as the basis for the production;

(B) shall include the date on which the tangible things must be provided, which shall allow a reasonable period of time within which the tangible things can be assembled and made available;

(C) shall provide clear and conspicuous notice of the principles and procedures described in subsection (d);

(D) may only require the production of a tangible thing if such thing can be obtained with a subpoena duces tecum issued by a court of the United States in aid of a grand jury investigation or with any other order issued by a court of the United States directing the production of records or tangible things;

(E) shall not disclose that such order is issued for purposes of an investigation described in subsection (a); and

(F) in the case of an application described in subsection (b)(2)(C), shall—

(i) authorize the production on a daily basis of call detail records for a period not to exceed 180 days;

(ii) provide that an order for such production may be extended upon application under subsection (b) and the judicial finding under paragraph (1) of this subsection;

(iii) provide that the Government may require the prompt production of a first set of call detail records using the specific selection term that satisfies the standard required under subsection (b)(2)(C)(ii);

(iv) provide that the Government may require the prompt production of a second set of call detail records using session-identifying information or a telephone calling card number identified by the specific selection term used to produce call detail records under clause (iii);

(v) provide that, when produced, such records be in a form that will be useful to the Government;

(vi) direct each person the Government directs to produce call detail records under the order to furnish the Government forthwith all information, facilities, or technical assistance necessary to accomplish the production in such a manner as will protect the secrecy of the production and produce a minimum of interference with the services that such person is providing to each subject of the production; and

(vii) direct the Government to—

(I) adopt minimization procedures that require the prompt destruction of all call detail records produced under the order that the Government determines are not foreign intelligence information; and

(II) destroy all call detail records produced under the order as prescribed by such procedures.

(3) No order issued under this subsection may authorize the collection of tangible things without the use of a specific selection term that meets the requirements of subsection (b)(2).

(4) A denial of the application made under this subsection may be reviewed as provided in section 103.

(d)(1) No person shall disclose to any other person that the Federal Bureau of Investigation has sought or obtained tangible things pursuant to an order issued or an emergency production required under this section, other than to

(A) those persons to whom disclosure is necessary to comply with such order or such emergency production;

(B) an attorney to obtain legal advice or assistance with respect to the production of things in response to the order or the emergency production; or

(C) other persons as permitted by the Director of the Federal Bureau of Investigation or the designee of the Director.

(2)(A) A person to whom disclosure is made pursuant to paragraph (1) shall be subject to the nondisclosure requirements applicable to a person

to whom an order or emergency production is directed under this section in the same manner as such person.

(B) Any person who discloses to a person described in subparagraph (A), (B), or (C) of paragraph (1) that the Federal Bureau of Investigation has sought or obtained tangible things pursuant to an order or emergency production under this section shall notify such person of the nondisclosure requirements of this subsection.

(C) At the request of the Director of the Federal Bureau of Investigation or the designee of the Director, any person making or intending to make a disclosure under subparagraph (A) or (C) of paragraph (1) shall identify to the Director or such designee the person to whom such disclosure will be made or to whom such disclosure was made prior to the request.

(e)(1) No cause of action shall lie in any court against a person who—

(A) produces tangible things or provides information, facilities, or technical assistance in accordance with an order issued or an emergency production required under this section; or

(B) otherwise provides technical assistance to the Government under this section or to implement the amendments made to this section by the USA FREEDOM Act of 2015.

(2) A production or provision of information, facilities, or technical assistance described in paragraph (1) shall not be deemed to constitute a waiver of any privilege in any other proceeding or context.

(f)(1) In this subsection—

(A) the term “production order” means an order to produce any tangible thing under this section; and

(B) the term “nondisclosure order” means an order imposed under subsection (d).

(2)(A)(i) A person receiving a production order may challenge the legality of the production order or any nondisclosure order imposed in connection with the production order by filing a petition with the pool established by section 103(e)(1).

(ii) The presiding judge shall immediately assign a petition under clause (i) to 1 of the judges serving in the pool established by section 103(e)(1). Not later than 72 hours after the assignment of such petition, the assigned judge shall conduct an initial review of the petition. If the assigned judge determines that the petition is frivolous, the assigned judge shall immediately deny the petition and affirm the production order or nondisclosure

order. If the assigned judge determines the petition is not frivolous, the assigned judge shall promptly consider the petition in accordance with the procedures established under section 103(e)(2).

(iii) The assigned judge shall promptly provide a written statement for the record of the reasons for any determination under this subsection. Upon the request of the Government, any order setting aside a nondisclosure order shall be stayed pending review pursuant to paragraph (3).

(B) A judge considering a petition to modify or set aside a production order may grant such petition only if the judge finds that such order does not meet the requirements of this section or is otherwise unlawful. If the judge does not modify or set aside the production order, the judge shall immediately affirm such order, and order the recipient to comply therewith.

(C)(i) A judge considering a petition to modify or set aside a nondisclosure order may grant such petition only if the judge finds that there is no reason to believe that disclosure may endanger the national security of the United States, interfere with a criminal, counterterrorism, or counterintelligence investigation, interfere with diplomatic relations, or endanger the life or physical safety of any person.

(ii) If the judge denies a petition to modify or set aside a nondisclosure order, the recipient of such order shall be precluded for a period of 1 year from filing another such petition with respect to such nondisclosure order.

(iii) Redesignated (ii)

(D) Any production or nondisclosure order not explicitly modified or set aside consistent with this subsection shall remain in full effect.

(3) A petition for review of a decision under paragraph (2) to affirm, modify, or set aside an order by the Government or any person receiving such order shall be made to the court of review established under section 103(b), which shall have jurisdiction to consider such petitions. The court of review shall provide for the record a written statement of the reasons for its decision and, on petition by the Government or any person receiving such order for writ of certiorari, the record shall be transmitted under seal to the Supreme Court of the United States, which shall have jurisdiction to review such decision.

(4) Judicial proceedings under this subsection shall be concluded as expeditiously as possible. The record of proceedings, including petitions filed, orders granted, and statements of reasons for decision, shall be maintained under security measures established by the Chief Justice of the United States, in consultation with the Attorney General and the Director of National Intelligence.

(5) All petitions under this subsection shall be filed under seal. In any proceedings under this subsection, the court shall, upon request of the Government, review *ex parte* and *in camera* any Government submission, or portions thereof, which may include classified information.

(g) MINIMIZATION PROCEDURES.—

(1) IN GENERAL.—The Attorney General shall adopt, and update as appropriate, specific minimization procedures governing the retention and dissemination by the Federal Bureau of Investigation of any tangible things, or information therein, received by the Federal Bureau of Investigation in response to an order under this title.

(2) DEFINED.—In this section, the term “minimization procedures” means—

(A) specific procedures that are reasonably designed in light of the purpose and technique of an order for the production of tangible things, to minimize the retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information;

(B) procedures that require that nonpublicly available information, which is not foreign intelligence information, as defined in section 101(e)(1) of this title, shall not be disseminated in a manner that identifies any United States person, without such person’s consent, unless such person’s identity is necessary to understand foreign intelligence information or assess its importance; and

(C) notwithstanding subparagraphs (A) and (B), procedures that allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes.

(3) RULE OF CONSTRUCTION.—Nothing in this subsection shall limit the authority of the court established under section 103(a) to impose additional, particularized minimization procedures with regard to the

production, retention, or dissemination of nonpublicly available information concerning unconsenting United States persons, including additional, particularized procedures related to the destruction of information within a reasonable time period.

(h) USE OF INFORMATION.—Information acquired from tangible things received by the Federal Bureau of Investigation in response to an order under this title concerning any United States person may be used and disclosed by Federal officers and employees without the consent of the United States person only in accordance with the minimization procedures adopted pursuant to subsection (g). No otherwise privileged information acquired from tangible things received by the Federal Bureau of Investigation in accordance with the provisions of this title shall lose its privileged character. No information acquired from tangible things received by the Federal Bureau of Investigation in response to an order under this title may be used or disclosed by Federal officers or employees except for lawful purposes.

(i) EMERGENCY AUTHORITY FOR PRODUCTION OF TANGIBLE THINGS.—

(1) Notwithstanding any other provision of this section, the Attorney General may require the emergency production of tangible things if the Attorney General—

(A) reasonably determines that an emergency situation requires the production of tangible things before an order authorizing such production can with due diligence be obtained;

(B) reasonably determines that the factual basis for the issuance of an order under this section to approve such production of tangible things exists;

(C) informs, either personally or through a designee, a judge having jurisdiction under this section at the time the Attorney General requires the emergency production of tangible things that the decision has been made to employ the authority under this subsection; and

(D) makes an application in accordance with this section to a judge having jurisdiction under this section as soon as practicable, but not later than 7 days after the Attorney General requires the emergency production of tangible things under this subsection.

(2) If the Attorney General requires the emergency production of tangible things under paragraph (1), the Attorney General shall require that the minimization procedures required by this section for the issuance of a judicial order be followed.

(3) In the absence of a judicial order approving the production of tangible things under this subsection, the production shall terminate when the

information sought is obtained, when the application for the order is denied, or after the expiration of 7 days from the time the Attorney General begins requiring the emergency production of such tangible things, whichever is earliest.

(4) A denial of the application made under this subsection may be reviewed as provided in section 103.

(5) If such application for approval is denied, or in any other case where the production of tangible things is terminated and no order is issued approving the production, no information obtained or evidence derived from such production shall be received in evidence or otherwise disclosed in any trial, hearing, or other proceeding in or before any court, grand jury, department, office, agency, regulatory body, legislative committee, or other authority of the United States, a State, or a political subdivision thereof, and no information concerning any United States person acquired from such production shall subsequently be used or disclosed in any other manner by Federal officers or employees without the consent of such person, except with the approval of the Attorney General if the information indicates a threat of death or serious bodily harm to any person.

(6) The Attorney General shall assess compliance with the requirements of paragraph (5).

(j) COMPENSATION.—The Government shall compensate a person for reasonable expenses incurred for—

(1) producing tangible things or providing information, facilities, or assistance in accordance with an order issued with respect to an application described in subsection (b)(2)(C) or an emergency production under subsection (i) that, to comply with subsection (i)(1)(D), requires an application described in subsection (b)(2)(C); or

(2) otherwise providing technical assistance to the Government under this section or to implement the amendments made to this section by the USA FREEDOM Act of 2015.

(k) DEFINITIONS.—In this section:

(1) IN GENERAL.—The terms “foreign power”, “agent of a foreign power”, “international terrorism”, “foreign intelligence information”, “Attorney General”, “United States person”, “United States”, “person”, and “State” have the meanings provided those terms in section 101.

(2) ADDRESS.—The term “address” means a physical address or electronic address, such as an electronic mail address or temporarily assigned network address (including an Internet protocol address).

(3) CALL DETAIL RECORD.—The term “call detail record”—

(A) means session-identifying information (including an originating or terminating telephone number, an International Mobile Subscriber Identity number, or an International Mobile Station Equipment Identity number), a telephone calling card number, or the time or duration of a call; and

(B) does not include—

(i) the contents (as defined in section 2510(8) of title 18, United States Code) of any communication;

(ii) the name, address, or financial information of a subscriber or customer; or

(iii) cell site location or global positioning system information.

(4) SPECIFIC SELECTION TERM.—

(A) TANGIBLE THINGS.—

(i) IN GENERAL.—Except as provided in subparagraph (B), a “specific selection term”—

(I) is a term that specifically identifies a person, account, address, or personal device, or any other specific identifier; and

(II) is used to limit, to the greatest extent reasonably practicable, the scope of tangible things sought consistent with the purpose for seeking the tangible things.

(ii) LIMITATION.—A specific selection term under clause (i) does not include an identifier that does not limit, to the greatest extent reasonably practicable, the scope of tangible things sought consistent with the purpose for seeking the tangible things, such as an identifier that—

(I) identifies an electronic communication service provider (as that term is defined in section 701) or a provider of remote computing service (as that term is defined in section 2711 of title 18, United States Code), when not used as part of a specific identifier as described in clause (i), unless the provider is itself a subject of an authorized investigation for which the specific selection term is used as the basis for the production; or

(II) identifies a broad geographic region, including the United States, a city, a county, a State, a zip code, or an area code, when not used

as part of a specific identifier as described in clause (i).

(iii) RULE OF CONSTRUCTION.—Nothing in this paragraph shall be construed to preclude the use of multiple terms or identifiers to meet the requirements of clause (i).

(B) CALL DETAIL RECORD APPLICATIONS.—For purposes of an application submitted under subsection (b)(2)(C), the term “specific selection term” means a term that specifically identifies an individual, account, or personal device.

CONGRESSIONAL OVERSIGHT

SEC. 502. [50 U.S.C. § 1862]

(a) On an annual basis, the Attorney General shall fully inform the Permanent Select Committee on Intelligence and the Committee on the Judiciary of the House of Representatives and the Select Committee on Intelligence and the Committee on the Judiciary of the House of Representatives and the Committee on the Judiciary of the Senate concerning all requests for the production of tangible things under section 501.

(b) In April of each year, the Attorney General shall submit to the House and Senate Committees on the Judiciary and the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence a report setting forth with respect to the preceding calendar year—

- (1) a summary of all compliance reviews conducted by the Government for the production of tangible things under section 501;
- (2) the total number of applications described in section 501(b)(2)(B) made for orders approving requests for the production of tangible things;
- (3) the total number of such orders either granted, modified, or denied;
- (4) the total number of applications described in section 501(b)(2)(C) made for orders approving requests for the production of call detail records;
- (5) the total number of such orders either granted, modified, or denied;
- (6) the total number of applications made for orders approving requests for the production of tangible things under section 501;
- (7) the total number of such orders either granted, modified, or denied; and
- (8) the number of such orders either granted, modified, or denied for the production of each of the following:
 - (A) Library circulation records, library patron lists, book sales records, or book customer lists.

- (B) Firearms sales records.
- (C) Tax return records.
- (D) Educational records.
- (E) Medical records containing information that would identify a person.

(c)(1) In April of each year, the Attorney General shall submit to Congress a report setting forth with respect to the preceding year—

- (A) the total number of applications made for orders approving requests for the production of tangible things under section 501;
- (B) the total number of such orders either granted, modified, or denied;
- (C) the total number of applications made for orders approving requests for the production of tangible things under section 501 in which the specific selection term does not specifically identify an individual, account, or personal device;
- (D) the total number of orders described in subparagraph (C) either granted, modified, or denied; and
- (E) with respect to orders described in subparagraph (D) that have been granted or modified, whether the court established under section 103 has directed additional, particularized minimization procedures beyond those adopted pursuant to section 501(g).

(2) Each report under this subsection shall be submitted in unclassified form.

TITLE 5, SECTION 552, UNITED STATES CODE
(THE "FREEDOM OF INFORMATION ACT")

**PUBLIC INFORMATION; AGENCY RULES, OPINIONS, ORDERS,
RECORDS, AND PROCEEDINGS**

SECTION 552.

(a) Each agency shall make available to the public information as follows:

(1) Each agency shall separately state and currently publish in the Federal Register for the guidance of the public—

(A) descriptions of its central and field organization and the established places at which, the employees (and in the case of a uniformed service, the members) from whom, and the methods whereby, the public may obtain information, make submittals or requests, or obtain decisions;

(B) statements of the general course and method by which its functions are channeled and determined, including the nature and requirements of all formal and informal procedures available;

(C) rules of procedure, descriptions of forms available or the places at which forms may be obtained, and instructions as to the scope and contents of all papers, reports, or examinations;

(D) substantive rules of general applicability adopted as authorized by law, and statements of general policy or interpretations of general applicability formulated and adopted by the agency; and

(E) each amendment, revision, or repeal of the foregoing.

Except to the extent that a person has actual and timely notice of the terms thereof, a person may not in any manner be required to resort to, or be adversely affected by, a matter required to be published in the Federal Register and not so published. For the purpose of this paragraph, matter reasonably available to the class of persons affected thereby is deemed published in the Federal Register when incorporated by reference therein with the approval of the Director of the Federal Register.

(2) Each agency, in accordance with published rules, shall make available for public inspection in an electronic format—

(A) final opinions, including concurring and dissenting opinions, as well as orders, made in the adjudication of cases;

(B) those statements of policy and interpretations which have been adopted by the agency and are not published in the Federal Register;

FREEDOM OF INFORMATION ACT

- (C) administrative staff manuals and instructions to staff that affect a member of the public;
- (D) copies of all records, regardless of form or format—
 - (i) that have been released to any person under paragraph (3); and
 - (ii)(I) that because of the nature of their subject matter, the agency determines have become or are likely to become the subject of subsequent requests for substantially the same records; or
 - (II) that have been requested 3 or more times;and
- (E) a general index of the records referred to under subparagraph (D);

unless the materials are promptly published and copies offered for sale. For records created on or after November 1, 1996, within one year after such date, each agency shall make such records available, including by computer telecommunications or, if computer telecommunications means have not been established by the agency, by other electronic means. To the extent required to prevent a clearly unwarranted invasion of personal privacy, an agency may delete identifying details when it makes available or publishes an opinion, statement of policy, interpretation, staff manual, instruction, or copies of records referred to in subparagraph (D). However, in each case the justification for the deletion shall be explained fully in writing, and the extent of such deletion shall be indicated on the portion of the record which is made available or published, unless including that indication would harm an interest protected by the exemption in subsection (b) under which the deletion is made. If technically feasible, the extent of the deletion shall be indicated at the place in the record where the deletion was made. Each agency shall also maintain and make available for public inspection in an electronic format current indexes providing identifying information for the public as to any matter issued, adopted, or promulgated after July 4, 1967, and required by this paragraph to be made available or published. Each agency shall promptly publish, quarterly or more frequently, and distribute (by sale or otherwise) copies of each index or supplements thereto unless it determines by order published in the Federal Register that the publication would be unnecessary and impracticable, in which case the agency shall nonetheless provide copies of such index on request at a cost not to exceed the direct cost of duplication. Each agency shall make the index referred to in subparagraph (E) available by computer telecommunications by December 31, 1999. A final order,

opinion, statement of policy, interpretation, or staff manual or instruction that affects a member of the public may be relied on, used, or cited as precedent by an agency against a party other than an agency only if—

- (i) it has been indexed and either made available or published as provided by this paragraph; or
- (ii) the party has actual and timely notice of the terms thereof.

(3)(A) Except with respect to the records made available under paragraphs (1) and (2) of this subsection, and except as provided in subparagraph (E), each agency, upon any request for records which (i) reasonably describes such records and (ii) is made in accordance with published rules stating the time, place, fees (if any), and procedures to be followed, shall make the records promptly available to any person.

(B) In making any record available to a person under this paragraph, an agency shall provide the record in any form or format requested by the person if the record is readily reproducible by the agency in that form or format. Each agency shall make reasonable efforts to maintain its records in forms or formats that are reproducible for purposes of this section.

(C) In responding under this paragraph to a request for records, an agency shall make reasonable efforts to search for the records in electronic form or format, except when such efforts would significantly interfere with the operation of the agency's automated information system.

(D) For purposes of this paragraph, the term "search" means to review, manually or by automated means, agency records for the purpose of locating those records which are responsive to a request.

(E) An agency, or part of an agency, that is an element of the intelligence community (as that term is defined in section 3(4) of the National Security Act of 1947 (50 U.S.C. 401a(4))) shall not make any record available under this paragraph to—

- (i) any government entity, other than a State, territory, commonwealth, or district of the United States, or any subdivision thereof; or
- (ii) a representative of a government entity described in clause (i).

(4)(A)(i) In order to carry out the provisions of this section, each agency shall promulgate regulations, pursuant to notice and receipt of public comment, specifying the schedule of fees applicable to the processing of requests under this section and establishing procedures and guidelines for determining when such fees should be waived or reduced. Such schedule

shall conform to the guidelines which shall be promulgated, pursuant to notice and receipt of public comment, by the Director of the Office of Management and Budget and which shall provide for a uniform schedule of fees for all agencies.

(ii) Such agency regulations shall provide that—

(I) fees shall be limited to reasonable standard charges for document search, duplication, and review, when records are requested for commercial use;

(II) fees shall be limited to reasonable standard charges for document duplication when records are not sought for commercial use and the request is made by an educational or noncommercial scientific institution, whose purpose is scholarly or scientific research; or a representative of the news media; and

(III) for any request not described in (I) or (II), fees shall be limited to reasonable standard charges for document search and duplication.

In this clause, the term “a representative of the news media” means any person or entity that gathers information of potential interest to a segment of the public, uses its editorial skills to turn the raw materials into a distinct work, and distributes that work to an audience. In this clause, the term “news” means information that is about current events or that would be of current interest to the public. Examples of news-media entities are television or radio stations broadcasting to the public at large and publishers of periodicals (but only if such entities qualify as disseminators of “news”) who make their products available for purchase by or subscription by or free distribution to the general public. These examples are not all-inclusive. Moreover, as methods of news delivery evolve (for example, the adoption of the electronic dissemination of newspapers through telecommunications services), such alternative media shall be considered to be news-media entities. A freelance journalist shall be regarded as working for a news-media entity if the journalist can demonstrate a solid basis for expecting publication through that entity,

whether or not the journalist is actually employed by the entity. A publication contract would present a solid basis for such an expectation; the Government may also consider the past publication record of the requester in making such a determination.

(iii) Documents shall be furnished without any charge or at a charge reduced below the fees established under clause (ii) if disclosure of the information is in the public interest because it is likely to contribute significantly to public understanding of the operations or activities of the government and is not primarily in the commercial interest of the requester.

(iv) Fee schedules shall provide for the recovery of only the direct costs of search, duplication, or review. Review costs shall include only the direct costs incurred during the initial examination of a document for the purposes of determining whether the documents must be disclosed under this section and for the purposes of withholding any portions exempt from disclosure under this section. Review costs may not include any costs incurred in resolving issues of law or policy that may be raised in the course of processing a request under this section. No fee may be charged by any agency under this section—

(I) if the costs of routine collection and processing of the fee are likely to equal or exceed the amount of the fee; or

(II) for any request described in clause (ii)(II) or (III) of this subparagraph for the first two hours of search time or for the first one hundred pages of duplication.

(v) No agency may require advance payment of any fee unless the requester has previously failed to pay fees in a timely fashion, or the agency has determined that the fee will exceed \$250.

(vi) Nothing in this subparagraph shall supersede fees chargeable under a statute specifically providing for setting the level of fees for particular types of records.

(vii) In any action by a requester regarding the waiver of fees under this section, the court shall determine the matter de novo: Provided, That the court's review of the matter shall be limited to the record before the agency.

(viii)(I) Except as provided in subclause (II), an agency shall not assess any search fees (or in the case of a requester described under clause (ii)(II) of this subparagraph, duplication fees) under this subparagraph if the agency has failed to comply with any time limit under paragraph (6).

(II)(aa) If an agency has determined that unusual circumstances apply (as the term is defined in paragraph (6)(B)) and the agency provided a timely written notice to the requester in accordance with paragraph (6)(B), a failure described in subclause (I) is excused for an additional 10 days. If the agency fails to comply with the extended time limit, the agency may not assess any search fees (or in the case of a requester described under clause (ii)(II) of this subparagraph, duplication fees).

(bb) If an agency has determined that unusual circumstances apply and more than 5,000 pages are necessary to respond to the request, an agency may charge search fees (or in the case of a requester described under clause (ii)(II) of this subparagraph, duplication fees) if the agency has provided a timely written notice to the requester in accordance with paragraph (6)(B) and the agency has discussed with the requester via written mail, electronic mail, or telephone (or made not less than 3 good-faith attempts to do so) how the requester could effectively limit the scope of the request in accordance with paragraph (6)(B)(ii).

(cc) If a court has determined that exceptional circumstances exist (as that term is defined in paragraph (6)(C)), a failure described in subclause (I) shall be excused for the length of time provided by the court order.

(B) On complaint, the district court of the United States in the district in which the complainant resides, or has his principal place of business, or in which the agency records are situated, or in the District of Columbia, has jurisdiction to enjoin the agency from withholding agency records and to order the production of any agency records improperly withheld from the complainant. In such a case the court shall determine the matter de novo, and may examine the contents of such agency records in camera to determine whether such records or any part thereof shall be withheld under any of the exemptions set forth in subsection (b) of this section, and the burden is on the agency to sustain its action. In addition to any other matters to which a court accords substantial weight, a court shall accord substantial weight to an affidavit of an agency concerning the agency's determination as to technical feasibility under paragraph (2)(C) and subsection (b) and reproducibility under paragraph (3)(B).

(C) Notwithstanding any other provision of law, the defendant shall serve an answer or otherwise plead to any complaint made under this subsection within thirty days after service upon the defendant of the pleading in which such complaint is made, unless the court otherwise directs for good cause shown.

[(D) Repealed.]

(E)(i) The court may assess against the United States reasonable attorney fees and other litigation costs reasonably incurred in any case under this section in which the complainant has substantially prevailed.

(ii) For purposes of this subparagraph, a complainant has substantially prevailed if the complainant has obtained relief through either—

(I) a judicial order, or an enforceable written agreement or consent decree; or

(II) a voluntary or unilateral change in position by the agency, if the complainant's claim is not insubstantial.

(F)(i) Whenever the court orders the production of any agency records improperly withheld from the complainant and assesses against the United States reasonable attorney fees and other litigation costs, and the court additionally issues a written finding that the circumstances surrounding the withholding raise questions whether agency personnel acted arbitrarily or capriciously with respect to the withholding, the Special Counsel

shall promptly initiate a proceeding to determine whether disciplinary action is warranted against the officer or employee who was primarily responsible for the withholding. The Special Counsel, after investigation and consideration of the evidence submitted, shall submit his findings and recommendations to the administrative authority of the agency concerned and shall send copies of the findings and recommendations to the officer or employee or his representative. The administrative authority shall take the corrective action that the Special Counsel recommends.

(ii) The Attorney General shall—

(I) notify the Special Counsel of each civil action described under the first sentence of clause (i); and

(II) annually submit a report to Congress on the number of such civil actions in the preceding year.

(iii) The Special Counsel shall annually submit a report to Congress on the actions taken by the Special Counsel under clause (i).

(G) In the event of noncompliance with the order of the court, the district court may punish for contempt the responsible employee, and in the case of a uniformed service, the responsible member.

(5) Each agency having more than one member shall maintain and make available for public inspection a record of the final votes of each member in every agency proceeding.

(6)(A) Each agency, upon any request for records made under paragraph (1), (2), or (3) of this subsection, shall—

(i) determine within 20 days (excepting Saturdays, Sundays, and legal public holidays) after the receipt of any such request whether to comply with such request and shall immediately notify the person making such request of—

(I) such determination and the reasons therefor;
(II) the right of such person to seek assistance from the FOIA Public Liaison of the agency;
and

(III) in the case of an adverse determination—
(aa) the right of such person to appeal to the head of the agency, within a period

determined by the head of the agency that is not less than 90 days after the date of such adverse determination; and (bb) the right of such person to seek dispute resolution services from the FOIA Public Liaison of the agency or the Office of Government Information Services; and

(ii) make a determination with respect to any appeal within twenty days (excepting Saturdays, Sundays, and legal public holidays) after the receipt of such appeal. If on appeal the denial of the request for records is in whole or in part upheld, the agency shall notify the person making such request of the provisions for judicial review of that determination under paragraph (4) of this subsection.

The 20-day period under clause (i) shall commence on the date on which the request is first received by the appropriate component of the agency, but in any event not later than ten days after the request is first received by any component of the agency that is designated in the agency's regulations under this section to receive requests under this section. The 20-day period shall not be tolled by the agency except—

(I) that the agency may make one request to the requester for information and toll the 20-day period while it is awaiting such information that it has reasonably requested from the requester under this section; or

(II) if necessary to clarify with the requester issues regarding fee assessment. In either case, the agency's receipt of the requester's response to the agency's request for information or clarification ends the tolling period.

(B)(i) In unusual circumstances as specified in this subparagraph, the time limits prescribed in either clause (i) or clause (ii) of subparagraph (A) may be extended by written notice to the person making such request setting forth the unusual circumstances for such extension and the date on which a determination is expected to be dispatched. No such notice shall specify a date that would result in an extension for more

than ten working days, except as provided in clause (ii) of this subparagraph.

(ii) With respect to a request for which a written notice under clause (i) extends the time limits prescribed under clause (i) of subparagraph (A), the agency shall notify the person making the request if the request cannot be processed within the time limit specified in that clause and shall provide the person an opportunity to limit the scope of the request so that it may be processed within that time limit or an opportunity to arrange with the agency an alternative time frame for processing the request or a modified request. To aid the requester, each agency shall make available its FOIA Public Liaison, who shall assist in the resolution of any disputes between the requester and the agency, and notify the requester of the right of the requester to seek dispute resolution services from the Office of Government Information Services. Refusal by the person to reasonably modify the request or arrange such an alternative time frame shall be considered as a factor in determining whether exceptional circumstances exist for purposes of subparagraph (C).

(iii) As used in this subparagraph, “unusual circumstances” means, but only to the extent reasonably necessary to the proper processing of the particular requests—

- (I) the need to search for and collect the requested records from field facilities or other establishments that are separate from the office processing the request;
- (II) the need to search for, collect, and appropriately examine a voluminous amount of separate and distinct records which are demanded in a single request; or
- (III) the need for consultation, which shall be conducted with all practicable speed, with another agency having a substantial interest in the determination of the request or among two or more components of the agency having substantial subject-matter interest therein.

(iv) Each agency may promulgate regulations, pursuant to notice and receipt of public comment, providing for the aggregation of certain requests by the same requestor, or by a group of requestors acting in concert, if the agency reasonably believes that such requests actually constitute a single request, which would otherwise satisfy the unusual circumstances specified in this subparagraph, and the requests involve clearly related matters. Multiple requests involving unrelated matters shall not be aggregated.

(C)(i) Any person making a request to any agency for records under paragraph (1), (2), or (3) of this subsection shall be deemed to have exhausted his administrative remedies with respect to such request if the agency fails to comply with the applicable time limit provisions of this paragraph. If the Government can show exceptional circumstances exist and that the agency is exercising due diligence in responding to the request, the court may retain jurisdiction and allow the agency additional time to complete its review of the records. Upon any determination by an agency to comply with a request for records, the records shall be made promptly available to such person making such request. Any notification of denial of any request for records under this subsection shall set forth the names and titles or positions of each person responsible for the denial of such request.

(ii) For purposes of this subparagraph, the term “exceptional circumstances” does not include a delay that results from a predictable agency workload of requests under this section, unless the agency demonstrates reasonable progress in reducing its backlog of pending requests.

(iii) Refusal by a person to reasonably modify the scope of a request or arrange an alternative time frame for processing a request (or a modified request) under clause (ii) after being given an opportunity to do so by the agency to whom the person made the request shall be considered as a factor in determining whether exceptional circumstances exist for purposes of this subparagraph.

(D)(i) Each agency may promulgate regulations, pursuant to notice and receipt of public comment, providing for multitrack

processing of requests for records based on the amount of work or time (or both) involved in processing requests.

(ii) Regulations under this subparagraph may provide a person making a request that does not qualify for the fastest multitrack processing an opportunity to limit the scope of the request in order to qualify for faster processing.

(iii) This subparagraph shall not be considered to affect the requirement under subparagraph (C) to exercise due diligence.

(E)(i) Each agency shall promulgate regulations, pursuant to notice and receipt of public comment, providing for expedited processing of requests for records—

(I) in cases in which the person requesting the records demonstrates a compelling need; and

(II) in other cases determined by the agency.

(ii) Notwithstanding clause (i), regulations under this subparagraph must ensure—

(I) that a determination of whether to provide expedited processing shall be made, and notice of the determination shall be provided to the person making the request, within 10 days after the date of the request; and

(II) expeditious consideration of administrative appeals of such determinations of whether to provide expedited processing.

(iii) An agency shall process as soon as practicable any request for records to which the agency has granted expedited processing under this subparagraph. Agency action to deny or affirm denial of a request for expedited processing pursuant to this subparagraph, and failure by an agency to respond in a timely manner to such a request shall be subject to judicial review under paragraph (4), except that the judicial review shall be based on the record before the agency at the time of the determination.

(iv) A district court of the United States shall not have jurisdiction to review an agency denial of expedited processing of a request for records after the agency has provided a complete response to the request.

(v) For purposes of this subparagraph, the term “compelling need” means—

(I) that a failure to obtain requested records on an expedited basis under this paragraph could reasonably be expected to pose an imminent threat to the life or physical safety of an individual; or

(II) with respect to a request made by a person primarily engaged in disseminating information, urgency to inform the public concerning actual or alleged Federal Government activity.

(vi) A demonstration of a compelling need by a person making a request for expedited processing shall be made by a statement certified by such person to be true and correct to the best of such person’s knowledge and belief.

(F) In denying a request for records, in whole or in part, an agency shall make a reasonable effort to estimate the volume of any requested matter the provision of which is denied, and shall provide any such estimate to the person making the request, unless providing such estimate would harm an interest protected by the exemption in subsection (b) pursuant to which the denial is made.

(7) Each agency shall—

(A) establish a system to assign an individualized tracking number for each request received that will take longer than ten days to process and provide to each person making a request the tracking number assigned to the request; and

(B) establish a telephone line or Internet service that provides information about the status of a request to the person making the request using the assigned tracking number, including—

(i) the date on which the agency originally received the request; and

(ii) an estimated date on which the agency will complete action on the request.

(8)(A) An agency shall—

(i) withhold information under this section only if—

(I) the agency reasonably foresees that disclosure would harm an interest protected by an exemption described in subsection (b); or

(II) disclosure is prohibited by law; and

(ii)(I) consider whether partial disclosure of information is possible whenever the agency determines that a full disclosure of a requested record is not possible; and

(II) take reasonable steps necessary to segregate and release nonexempt information; and

(B) Nothing in this paragraph requires disclosure of information that is otherwise prohibited from disclosure by law, or otherwise exempted from disclosure under subsection (b)(3).

(b) This section does not apply to matters that are—

(1)(A) specifically authorized under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy and (B) are in fact properly classified pursuant to such Executive order;

(2) related solely to the internal personnel rules and practices of an agency;

(3) specifically exempted from disclosure by statute (other than section 552b of this title), if that statute—

(A)(i) requires that the matters be withheld from the public in such a manner as to leave no discretion on the issue; or

(ii) establishes particular criteria for withholding or refers to particular types of matters to be withheld; and

(B) if enacted after the date of enactment of the OPEN FOIA Act of 2009, specifically cites to this paragraph.

(4) trade secrets and commercial or financial information obtained from a person and privileged or confidential;

(5) inter-agency or intra-agency memorandums or letters that would not be available by law to a party other than an agency in litigation with the agency, provided that the deliberative process privilege shall not apply to records created 25 years or more before the date on which the records were requested;

(6) personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy;

(7) records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information (A) could reasonably be expected to interfere with enforcement proceedings, (B) would deprive a person of a right to a fair trial or an impartial adjudication, (C) could reasonably be expected to constitute an unwarranted invasion of personal privacy, (D) could reasonably be expected to disclose the identity of a confidential source, including a State, local, or foreign agency or authority or any private institution which furnished information on a confidential basis, and, in the case of a record or information compiled by criminal law

enforcement authority in the course of a criminal investigation or by an agency conducting a lawful national security intelligence investigation, information furnished by a confidential source, (E) would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law, or (F) could reasonably be expected to endanger the life or physical safety of any individual; (8) contained in or related to examination, operating, or condition reports prepared by, on behalf of, or for the use of an agency responsible for the regulation or supervision of financial institutions; or (9) geological and geophysical information and data, including maps, concerning wells.

Any reasonably segregable portion of a record shall be provided to any person requesting such record after deletion of the portions which are exempt under this subsection. The amount of information deleted, and the exemption under which the deletion is made, shall be indicated on the released portion of the record, unless including that indication would harm an interest protected by the exemption in this subsection under which the deletion is made. If technically feasible, the amount of the information deleted, and the exemption under which the deletion is made, shall be indicated at the place in the record where such deletion is made.

(c)(1) Whenever a request is made which involves access to records described in subsection (b)(7)(A) and—

(A) the investigation or proceeding involves a possible violation of criminal law; and

(B) there is reason to believe that (i) the subject of the investigation or proceeding is not aware of its pendency, and (ii) disclosure of the existence of the records could reasonably be expected to interfere with enforcement proceedings,

the agency may, during only such time as that circumstance continues, treat the records as not subject to the requirements of this section.

(2) Whenever informant records maintained by a criminal law enforcement agency under an informant's name or personal identifier are requested by a third party according to the informant's name or personal identifier, the agency may treat the records as not subject to the requirements of this section unless the informant's status as an informant has been officially confirmed.

(3) Whenever a request is made which involves access to records maintained by the Federal Bureau of Investigation pertaining to foreign intelligence or counterintelligence, or international terrorism, and the

FREEDOM OF INFORMATION ACT

existence of the records is classified information as provided in subsection (b)(1), the Bureau may, as long as the existence of the records remains classified information, treat the records as not subject to the requirements of this section.

(d) This section does not authorize withholding of information or limit the availability of records to the public, except as specifically stated in this section. This section is not authority to withhold information from Congress.

(e)(1) On or before February 1 of each year, each agency shall submit to the Attorney General of the United States and to the Director of the Office of Government Information Services a report which shall cover the preceding fiscal year and which shall include—

- (A) the number of determinations made by the agency not to comply with requests for records made to such agency under subsection (a) and the reasons for each such determination;
- (B)(i) the number of appeals made by persons under subsection (a)(6), the result of such appeals, and the reason for the action upon each appeal that results in a denial of information; and
 - (ii) a complete list of all statutes that the agency relies upon to authorize the agency to withhold information under subsection (b)(3), the number of occasions on which each statute was relied upon, a description of whether a court has upheld the decision of the agency to withhold information under each such statute, and a concise description of the scope of any information withheld;
- (C) the number of requests for records pending before the agency as of September 30 of the preceding year, and the median and average number of days that such requests had been pending before the agency as of that date;
- (D) the number of requests for records received by the agency and the number of requests which the agency processed;
- (E) the median number of days taken by the agency to process different types of requests, based on the date on which the requests were received by the agency;
- (F) the average number of days for the agency to respond to a request beginning on the date on which the request was received by the agency, the median number of days for the agency to respond to such requests, and the range in number of days for the agency to respond to such requests;
- (G) based on the number of business days that have elapsed since each request was originally received by the agency—

- (i) the number of requests for records to which the agency has responded with a determination within a period up to and including 20 days, and in 20-day increments up to and including 200 days;
 - (ii) the number of requests for records to which the agency has responded with a determination within a period greater than 200 days and less than 301 days;
 - (iii) the number of requests for records to which the agency has responded with a determination within a period greater than 300 days and less than 401 days; and
 - (iv) the number of requests for records to which the agency has responded with a determination within a period greater than 400 days;
- (H) the average number of days for the agency to provide the granted information beginning on the date on which the request was originally filed, the median number of days for the agency to provide the granted information, and the range in number of days for the agency to provide the granted information;
- (I) the median and average number of days for the agency to respond to administrative appeals based on the date on which the appeals originally were received by the agency, the highest number of business days taken by the agency to respond to an administrative appeal, and the lowest number of business days taken by the agency to respond to an administrative appeal;
- (J) data on the 10 active requests with the earliest filing dates pending at each agency, including the amount of time that has elapsed since each request was originally received by the agency;
- (K) data on the 10 active administrative appeals with the earliest filing dates pending before the agency as of September 30 of the preceding year, including the number of business days that have elapsed since the requests were originally received by the agency;
- (L) the number of expedited review requests that are granted and denied, the average and median number of days for adjudicating expedited review requests, and the number adjudicated within the required 10 days;
- (M) the number of fee waiver requests that are granted and denied, and the average and median number of days for adjudicating fee waiver determinations;

FREEDOM OF INFORMATION ACT

- (N) the total amount of fees collected by the agency for processing requests;
 - (O) the number of full-time staff of the agency devoted to processing requests for records under this section, and the total amount expended by the agency for processing such requests;
 - (P) the number of times the agency denied a request for records under subsection (c); and
 - (Q) the number of records that were made available for public inspection in an electronic format under subsection (a)(2).
- (2) Information in each report submitted under paragraph (1) shall be expressed in terms of each principal component of the agency and for the agency overall.
- (3) Each agency shall make each such report available for public inspection in an electronic format. In addition, each agency shall make the raw statistical data used in each report available in a timely manner for public inspection in an electronic format, which shall be made available—
- (A) without charge, license, or registration requirement;
 - (B) in an aggregated, searchable format; and
 - (C) in a format that may be downloaded in bulk.
- (4) The Attorney General of the United States shall make each report which has been made available by electronic means available at a single electronic access point. The Attorney General of the United States shall notify the Chairman and ranking minority member of the Committee on Oversight and Government Reform of the House of Representatives and the Chairman and ranking minority member of the Committees on Homeland Security and Governmental Affairs and the Judiciary of the Senate, no later than March 1 of the year in which each such report is issued, that such reports are available by electronic means.
- (5) The Attorney General of the United States, in consultation with the Director of the Office of Management and Budget, shall develop reporting and performance guidelines in connection with reports required by this subsection by October 1, 1997, and may establish additional requirements for such reports as the Attorney General determines may be useful.
- (6)(A) The Attorney General of the United States shall submit to the Committee on Oversight and Government Reform of the House of Representatives, the Committee on the Judiciary of the Senate, and the President a report on or before March 1 of each calendar year, which shall include for the prior calendar year—

- (i) a listing of the number of cases arising under this section;
 - (ii) a listing of—
 - (I) each subsection, and any exemption, if applicable, involved in each case arising under this section;
 - (II) the disposition of each case arising under this section; and
 - (III) the cost, fees, and penalties assessed under subparagraphs (E), (F), and (G) of subsection (a)(4); and
 - (iii) a description of the efforts undertaken by the Department of Justice to encourage agency compliance with this section.
- (B) The Attorney General of the United States shall make—
- (i) each report submitted under subparagraph (A) available for public inspection in an electronic format; and
 - (ii) the raw statistical data used in each report submitted under subparagraph (A) available for public inspection in an electronic format, which shall be made available—
 - (I) without charge, license, or registration requirement;
 - (II) in an aggregated, searchable format; and
 - (III) in a format that may be downloaded in bulk.

(f) For purposes of this section, the term—

- (1) “agency” as defined in section 551(1) of this title includes any executive department, military department, Government corporation, Government controlled corporation, or other establishment in the executive branch of the Government (including the Executive Office of the President), or any independent regulatory agency; and
- (2) “record” and any other term used in this section in reference to information includes—

- (A) any information that would be an agency record subject to the requirements of this section when maintained by an agency in any format, including an electronic format; and
- (B) any information described under subparagraph (A) that is maintained for an agency by an entity under Government contract, for the purposes of records management.

FREEDOM OF INFORMATION ACT

(g) The head of each agency shall prepare and make available for public inspection in an electronic format, reference material or a guide for requesting records or information from the agency, subject to the exemptions in subsection (b), including—

- (1) an index of all major information systems of the agency;
- (2) a description of major information and record locator systems maintained by the agency; and
- (3) a handbook for obtaining various types and categories of public information from the agency pursuant to chapter 35 of title 44, and under this section.

(h)(1) There is established the Office of Government Information Services within the National Archives and Records Administration. The head of the Office shall be the Director of the Office of Government Information Services.

(2) The Office of Government Information Services shall—

- (A) review policies and procedures of administrative agencies under this section;
- (B) review compliance with this section by administrative agencies; and
- (C) identify procedures and methods for improving compliance under this section.

(3) The Office of Government Information Services shall offer mediation services to resolve disputes between persons making requests under this section and administrative agencies as a nonexclusive alternative to litigation and may issue advisory opinions at the discretion of the Office or upon request of any party to a dispute.

(4)(A) Not less frequently than annually, the Director of the Office of Government Information Services shall submit to the Committee on Oversight and Government Reform of the House of Representatives, the Committee on the Judiciary of the Senate, and the President—

(i) a report on the findings of the information reviewed and identified under paragraph (2);

(ii) a summary of the activities of the Office of Government Information Services under paragraph (3), including—

- (I) any advisory opinions issued; and
- (II) the number of times each agency engaged in dispute resolution with the assistance of the Office of Government Information Services or the FOIA Public Liaison; and

(iii) legislative and regulatory recommendations, if any, to improve the administration of this section.

(B) The Director of the Office of Government Information Services shall make each report submitted under subparagraph (A) available for public inspection in an electronic format.

(C) The Director of the Office of Government Information Services shall not be required to obtain the prior approval, comment, or review of any officer or agency of the United States, including the Department of Justice, the Archivist of the United States, or the Office of Management and Budget before submitting to Congress, or any committee or subcommittee thereof, any reports, recommendations, testimony, or comments, if such submissions include a statement indicating that the views expressed therein are those of the Director and do not necessarily represent the views of the President.

(5) The Director of the Office of Government Information Services may directly submit additional information to Congress and the President as the Director determines to be appropriate.

(6) Not less frequently than annually, the Office of Government Information Services shall conduct a meeting that is open to the public on the review and reports by the Office and shall allow interested persons to appear and present oral or written statements at the meeting.

(i) The Government Accountability Office shall conduct audits of administrative agencies on the implementation of this section and issue reports detailing the results of such audits.

(j)(1) Each agency shall designate a Chief FOIA Officer who shall be a senior official of such agency (at the Assistant Secretary or equivalent level).

(2) The Chief FOIA Officer of each agency shall, subject to the authority of the head of the agency—

(A) have agency-wide responsibility for efficient and appropriate compliance with this section;

(B) monitor implementation of this section throughout the agency and keep the head of the agency, the chief legal officer of the agency, and the Attorney General appropriately informed of the agency's performance in implementing this section;

(C) recommend to the head of the agency such adjustments to agency practices, policies, personnel, and funding as may be necessary to improve its implementation of this section;

(D) review and report to the Attorney General, through the head of the agency, at such times and in such formats as the Attorney General may direct, on the agency's performance in implementing this section;

(E) facilitate public understanding of the purposes of the statutory exemptions of this section by including concise descriptions of the exemptions in both the agency's handbook issued under subsection (g), and the agency's annual report on this section, and by providing an overview, where appropriate, of certain general categories of agency records to which those exemptions apply;

(F) offer training to agency staff regarding their responsibilities under this section;

(G) serve as the primary agency liaison with the Office of Government Information Services and the Office of Information Policy; and

(H) designate 1 or more FOIA Public Liaisons.

(3) The Chief FOIA Officer of each agency shall review, not less frequently than annually, all aspects of the administration of this section by the agency to ensure compliance with the requirements of this section, including—

(A) agency regulations;

(B) disclosure of records required under paragraphs (2) and (8) of subsection (a);

(C) assessment of fees and determination of eligibility for fee waivers;

(D) the timely processing of requests for information under this section;

(E) the use of exemptions under subsection (b); and

(F) dispute resolution services with the assistance of the Office of Government Information Services or the FOIA Public Liaison.

(k)(1) There is established in the executive branch the Chief FOIA Officers Council (referred to in this subsection as the "Council").

(2) The Council shall be comprised of the following members:

(A) The Deputy Director for Management of the Office of Management and Budget.

(B) The Director of the Office of Information Policy at the Department of Justice.

(C) The Director of the Office of Government Information Services.

(D) The Chief FOIA Officer of each agency.

(E) Any other officer or employee of the United States as designated by the Co-Chairs.

(3) The Director of the Office of Information Policy at the Department of Justice and the Director of the Office of Government Information Services shall be the Co-Chairs of the Council.

(4) The Administrator of General Services shall provide administrative and other support for the Council.

(5)(A) The duties of the Council shall include the following:

(i) Develop recommendations for increasing compliance and efficiency under this section.

(ii) Disseminate information about agency experiences, ideas, best practices, and innovative approaches related to this section.

(iii) Identify, develop, and coordinate initiatives to increase transparency and compliance with this section.

(iv) Promote the development and use of common performance measures for agency compliance with this section.

(B) In performing the duties described in subparagraph (A), the Council shall consult on a regular basis with members of the public who make requests under this section.

(6)(A) The Council shall meet regularly and such meetings shall be open to the public unless the Council determines to close the meeting for reasons of national security or to discuss information exempt under subsection (b).

(B) Not less frequently than annually, the Council shall hold a meeting that shall be open to the public and permit interested persons to appear and present oral and written statements to the Council.

(C) Not later than 10 business days before a meeting of the Council, notice of such meeting shall be published in the Federal Register.

(D) Except as provided in subsection (b), the records, reports, transcripts, minutes, appendices, working papers, drafts, studies, agenda, or other documents that were made available to or prepared for or by the Council shall be made publicly available.

(E) Detailed minutes of each meeting of the Council shall be kept and shall contain a record of the persons present, a complete and accurate description of matters discussed and conclusions reached, and copies of all reports received, issued, or approved by the Council. The minutes shall be redacted as necessary and made publicly available.

(l) FOIA Public Liaisons shall report to the agency Chief FOIA Officer and shall serve as supervisory officials to whom a requester under this section can raise concerns about the service the requester has received from the FOIA Requester Center, following an initial response from the FOIA Requester Center Staff. FOIA Public Liaisons shall be responsible for assisting in reducing delays, increasing transparency and understanding of the status of requests, and assisting in the resolution of disputes.

(m)(1) The Director of the Office of Management and Budget, in consultation with the Attorney General, shall ensure the operation of a consolidated online request portal that allows a member of the public to submit a request for records under subsection (a) to any agency from a single website. The portal may include any additional tools the Director of the Office of Management and Budget finds will improve the implementation of this section.

(2) This subsection shall not be construed to alter the power of any other agency to create or maintain an independent online portal for the submission of a request for records under this section. The Director of the Office of Management and Budget shall establish standards for interoperability between the portal required under paragraph (1) and other request processing software used by agencies subject to this section.

TITLE 5, SECTION 552A, UNITED STATES CODE
(THE "PRIVACY ACT")

RECORDS MAINTAINED ON INDIVIDUALS

SECTION 552a.

(a) DEFINITIONS.—For purposes of this section—

- (1) the term “agency” means agency as defined in section 552(e) of this title;
- (2) the term “individual” means a citizen of the United States or an alien lawfully admitted for permanent residence;
- (3) the term “maintain” includes maintain, collect, use, or disseminate;
- (4) the term “record” means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph;
- (5) the term “system of records” means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual;
- (6) the term “statistical record” means a record in a system of records maintained for statistical research or reporting purposes only and not used in whole or in part in making any determination about an identifiable individual, except as provided by section 8 of title 13;
- (7) the term “routine use” means, with respect to the disclosure of a record, the use of such record for a purpose which is compatible with the purpose for which it was collected;
- (8) the term “matching program”—
 - (A) means any computerized comparison of—
 - (i) two or more automated systems of records or a system of records with non-Federal records for the purpose of—
 - (I) establishing or verifying the eligibility of, or continuing compliance with statutory and regulatory requirements by, applicants for, recipients or beneficiaries of, participants in, or providers of services with respect to, cash or in-

PRIVACY ACT

- kind assistance or payments under Federal benefit programs, or
 - (II) recouping payments or delinquent debts under such Federal benefit programs, or
 - (ii) two or more automated Federal personnel or payroll systems of records or a system of Federal personnel or payroll records with non-Federal records,
- (B) but does not include—
- (i) matches performed to produce aggregate statistical data without any personal identifiers;
 - (ii) matches performed to support any research or statistical project, the specific data of which may not be used to make decisions concerning the rights, benefits, or privileges of specific individuals;
 - (iii) matches performed, by an agency (or component thereof) which performs as its principal function any activity pertaining to the enforcement of criminal laws, subsequent to the initiation of a specific criminal or civil law enforcement investigation of a named person or persons for the purpose of gathering evidence against such person or persons;
 - (iv) matches of tax information—
 - (I) pursuant to section 6103(d) of the Internal Revenue Code of 1986,
 - (II) for purposes of tax administration as defined in section 6103(b)(4) of such Code,
 - (III) for the purpose of intercepting a tax refund due an individual under authority granted by section 404(e), 464, or 1137 of the Social Security Act; or
 - (IV) for the purpose of intercepting a tax refund due an individual under any other tax refund intercept program authorized by statute which has been determined by the Director of the Office of Management and Budget to contain verification, notice, and hearing requirements that are substantially similar to the procedures in section 1137 of the Social Security Act;
 - (v) matches—
 - (I) using records predominantly relating to Federal personnel, that are performed for routine

PRIVACY ACT

administrative purposes (subject to guidance provided by the Director of the Office of Management and Budget pursuant to subsection (v)); or

(II) conducted by an agency using only records from systems of records maintained by that agency;

if the purpose of the match is not to take any adverse financial, personnel, disciplinary, or other adverse action against Federal personnel;

(vi) matches performed for foreign counterintelligence purposes or to produce background checks for security clearances of Federal personnel or Federal contractor personnel;

(vii) matches performed incident to a levy described in section 6103(k)(8) of the Internal Revenue Code of 1986;

(viii) matches performed pursuant to section 202(x)(3) or 1611(e)(1) of the Social Security Act (42 U.S.C. § 402(x)(3), 1382(e)(1));

(ix) matches performed by the Secretary of Health and Human Services or the Inspector General of the Department of Health and Human Services with respect to potential fraud, waste, and abuse, including matches of a system of records with non-Federal records; or

(x) matches performed pursuant to section 3(d)(4) of the Achieving a Better Life Experience Act of 2014;

(9) the term “recipient agency” means any agency, or contractor thereof, receiving records contained in a system of records from a source agency for use in a matching program;

(10) the term “non-Federal agency” means any State or local government, or agency thereof, which receives records contained in a system of records from a source agency for use in a matching program;

(11) the term “source agency” means any agency which discloses records contained in a system of records to be used in a matching program, or any State or local government, or agency thereof, which discloses records to be used in a matching program;

(12) the term “Federal benefit program” means any program administered or funded by the Federal Government, or by any agent or State on behalf of the Federal Government, providing cash or in-kind

PRIVACY ACT

assistance in the form of payments, grants, loans, or loan guarantees to individuals; and

(13) the term “Federal personnel” means officers and employees of the Government of the United States, members of the uniformed services (including members of the Reserve Components), individuals entitled to receive immediate or deferred retirement benefits under any retirement program of the Government of the United States (including survivor benefits).

(b) CONDITIONS OF DISCLOSURE.—No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains, unless disclosure of the record would be—

- (1) to those officers and employees of the agency which maintains the record who have a need for the record in the performance of their duties;
- (2) required under section 552 of this title;
- (3) for a routine use as defined in subsection (a)(7) of this section and described under subsection (e)(4)(D) of this section;
- (4) to the Bureau of the Census for purposes of planning or carrying out a census or survey or related activity pursuant to the provisions of title 13;
- (5) to a recipient who has provided the agency with advance adequate written assurance that the record will be used solely as a statistical research or reporting record, and the record is to be transferred in a form that is not individually identifiable;
- (6) to the National Archives and Records Administration as a record which has sufficient historical or other value to warrant its continued preservation by the United States Government, or for evaluation by the Archivist of the United States or the designee of the Archivist to determine whether the record has such value;
- (7) to another agency or to an instrumentality of any governmental jurisdiction within or under the control of the United States for a civil or criminal law enforcement activity if the activity is authorized by law, and if the head of the agency or instrumentality has made a written request to the agency which maintains the record specifying the particular portion desired and the law enforcement activity for which the record is sought;
- (8) to a person pursuant to a showing of compelling circumstances affecting the health or safety of an individual if upon such disclosure notification is transmitted to the last known address of such individual;
- (9) to either House of Congress, or, to the extent of matter within its jurisdiction, any committee or subcommittee thereof, any joint committee of Congress or subcommittee of any such joint committee;

PRIVACY ACT

(10) to the Comptroller General, or any of his authorized representatives, in the course of the performance of the duties of the Government Accountability Office;

(11) pursuant to the order of a court of competent jurisdiction; or

(12) to a consumer reporting agency in accordance with section 3711(e) of title 31.

(c) ACCOUNTING OF CERTAIN DISCLOSURES.—Each agency, with respect to each system of records under its control, shall—

(1) except for disclosures made under subsections (b)(1) or (b)(2) of this section, keep an accurate accounting of—

(A) the date, nature, and purpose of each disclosure of a record to any person or to another agency made under subsection (b) of this section; and

(B) the name and address of the person or agency to whom the disclosure is made;

(2) retain the accounting made under paragraph (1) of this subsection for at least five years or the life of the record, whichever is longer, after the disclosure for which the accounting is made;

(3) except for disclosures made under subsection (b)(7) of this section, make the accounting made under paragraph (1) of this subsection available to the individual named in the record at his request; and

(4) inform any person or other agency about any correction or notation of dispute made by the agency in accordance with subsection (d) of this section of any record that has been disclosed to the person or agency if an accounting of the disclosure was made.

(d) ACCESS TO RECORDS.—Each agency that maintains a system of records shall—

(1) upon request by any individual to gain access to his record or to any information pertaining to him which is contained in the system, permit him and upon his request, a person of his own choosing to accompany him, to review the record and have a copy made of all or any portion thereof in a form comprehensible to him, except that the agency may require the individual to furnish a written statement authorizing discussion of that individual's record in the accompanying person's presence;

(2) permit the individual to request amendment of a record pertaining to him and—

(A) not later than 10 days (excluding Saturdays, Sundays, and legal public holidays) after the date of receipt of such request, acknowledge in writing such receipt; and

(B) promptly, either—

(i) make any correction of any portion thereof which the individual believes is not accurate, relevant, timely, or complete; or

(ii) inform the individual of its refusal to amend the record in accordance with his request, the reason for the refusal, the procedures established by the agency for the individual to request a review of that refusal by the head of the agency or an officer designated by the head of the agency, and the name and business address of that official;

(3) permit the individual who disagrees with the refusal of the agency to amend his record to request a review of such refusal, and not later than 30 days (excluding Saturdays, Sundays, and legal public holidays) from the date on which the individual requests such review, complete such review and make a final determination unless, for good cause shown, the head of the agency extends such 30-day period; and if, after his review, the reviewing official also refuses to amend the record in accordance with the request, permit the individual to file with the agency a concise statement setting forth the reasons for his disagreement with the refusal of the agency, and notify the individual of the provisions for judicial review of the reviewing official's determination under subsection (g)(1)(A) of this section;

(4) in any disclosure, containing information about which the individual has filed a statement of disagreement, occurring after the filing of the statement under paragraph (3) of this subsection, clearly note any portion of the record which is disputed and provide copies of the statement and, if the agency deems it appropriate, copies of a concise statement of the reasons of the agency for not making the amendments requested, to persons or other agencies to whom the disputed record has been disclosed; and

(5) nothing in this section shall allow an individual access to any information compiled in reasonable anticipation of a civil action or proceeding.

(e) AGENCY REQUIREMENTS.—Each agency that maintains a system of records shall—

(1) maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by executive order of the President;

(2) collect information to the greatest extent practicable directly from the subject individual when the information may result in adverse

PRIVACY ACT

determinations about an individual's rights, benefits, and privileges under Federal programs;

(3) inform each individual whom it asks to supply information, on the form which it uses to collect the information or on a separate form that can be retained by the individual—

(A) the authority (whether granted by statute, or by executive order of the President) which authorizes the solicitation of the information and whether disclosure of such information is mandatory or voluntary;

(B) the principal purpose or purposes for which the information is intended to be used;

(C) the routine uses which may be made of the information, as published pursuant to paragraph (4)(D) of this subsection; and

(D) the effects on him, if any, of not providing all or any part of the requested information;

(4) subject to the provisions of paragraph (11) of this subsection, publish in the Federal Register upon establishment or revision a notice of the existence and character of the system of records, which notice shall include—

(A) the name and location of the system;

(B) the categories of individuals on whom records are maintained in the system;

(C) the categories of records maintained in the system;

(D) each routine use of the records contained in the system, including the categories of users and the purpose of such use;

(E) the policies and practices of the agency regarding storage, retrievability, access controls, retention, and disposal of the records;

(F) the title and business address of the agency official who is responsible for the system of records;

(G) the agency procedures whereby an individual can be notified at his request if the system of records contains a record pertaining to him;

(H) the agency procedures whereby an individual can be notified at his request how he can gain access to any record pertaining to him contained in the system of records, and how he can contest its content; and

(I) the categories of sources of records in the system;

(5) maintain all records which are used by the agency in making any determination about any individual with such accuracy, relevance,

timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination;

(6) prior to disseminating any record about an individual to any person other than an agency, unless the dissemination is made pursuant to subsection (b)(2) of this section, make reasonable efforts to assure that such records are accurate, complete, timely, and relevant for agency purposes;

(7) maintain no record describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual about whom the record is maintained or unless pertinent to and within the scope of an authorized law enforcement activity;

(8) make reasonable efforts to serve notice on an individual when any record on such individual is made available to any person under compulsory legal process when such process becomes a matter of public record;

(9) establish rules of conduct for persons involved in the design, development, operation, or maintenance of any system of records, or in maintaining any record, and instruct each such person with respect to such rules and the requirements of this section, including any other rules and procedures adopted pursuant to this section and the penalties for noncompliance;

(10) establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained;

(11) at least 30 days prior to publication of information under paragraph (4)(D) of this subsection, publish in the Federal Register notice of any new use or intended use of the information in the system, and provide an opportunity for interested persons to submit written data, views, or arguments to the agency; and

(12) if such agency is a recipient agency or a source agency in a matching program with a non-Federal agency, with respect to any establishment or revision of a matching program, at least 30 days prior to conducting such program, publish in the Federal Register notice of such establishment or revision.

(f) AGENCY RULES.—In order to carry out the provisions of this section, each agency that maintains a system of records shall promulgate rules, in accordance

PRIVACY ACT

with the requirements (including general notice) of section 553 of this title, which shall—

- (1) establish procedures whereby an individual can be notified in response to his request if any system of records named by the individual contains a record pertaining to him;
- (2) define reasonable times, places, and requirements for identifying an individual who requests his record or information pertaining to him before the agency shall make the record or information available to the individual;
- (3) establish procedures for the disclosure to an individual upon his request of his record or information pertaining to him, including special procedure, if deemed necessary, for the disclosure to an individual of medical records, including psychological records, pertaining to him;
- (4) establish procedures for reviewing a request from an individual concerning the amendment of any record or information pertaining to the individual, for making a determination on the request, for an appeal within the agency of an initial adverse agency determination, and for whatever additional means may be necessary for each individual to be able to exercise fully his rights under this section; and
- (5) establish fees to be charged, if any, to any individual for making copies of his record, excluding the cost of any search for and review of the record.

The Office of the Federal Register shall biennially compile and publish the rules promulgated under this subsection and agency notices published under subsection (e)(4) of this section in a form available to the public at low cost.

(g)(1) CIVIL REMEDIES.—Whenever any agency

- (A) makes a determination under subsection (d)(3) of this section not to amend an individual's record in accordance with his request, or fails to make such review in conformity with that subsection;
- (B) refuses to comply with an individual request under subsection (d)(1) of this section;
- (C) fails to maintain any record concerning any individual with such accuracy, relevance, timeliness, and completeness as is necessary to assure fairness in any determination relating to the qualifications, character, rights, or opportunities of, or benefits to the individual that may be made on the basis of such record, and consequently a determination is made which is adverse to the individual; or

(D) fails to comply with any other provision of this section, or any rule promulgated thereunder, in such a way as to have an adverse effect on an individual,

the individual may bring a civil action against the agency, and the district courts of the United States shall have jurisdiction in the matters under the provisions of this subsection.

(2)(A) In any suit brought under the provisions of subsection (g)(1)(A) of this section, the court may order the agency to amend the individual's record in accordance with his request or in such other way as the court may direct. In such a case the court shall determine the matter de novo.

(B) The court may assess against the United States reasonable attorney fees and other litigation costs reasonably incurred in any case under this paragraph in which the complainant has substantially prevailed.

(3)(A) In any suit brought under the provisions of subsection (g)(1)(B) of this section, the court may enjoin the agency from withholding the records and order the production to the complainant of any agency records improperly withheld from him. In such a case the court shall determine the matter de novo, and may examine the contents of any agency records in camera to determine whether the records or any portion thereof may be withheld under any of the exemptions set forth in subsection (k) of this section, and the burden is on the agency to sustain its action.

(B) The court may assess against the United States reasonable attorney fees and other litigation costs reasonably incurred in any case under this paragraph in which the complainant has substantially prevailed.

(4) In any suit brought under the provisions of subsection (g)(1)(C) or (D) of this section in which the court determines that the agency acted in a manner which was intentional or willful, the United States shall be liable to the individual in an amount equal to the sum of—

(A) actual damages sustained by the individual as a result of the refusal or failure, but in no case shall a person entitled to recovery receive less than the sum of \$1,000; and

(B) the costs of the action together with reasonable attorney fees as determined by the court.

(5) An action to enforce any liability created under this section may be brought in the district court of the United States in the district in which the complainant resides, or has his principal place of business, or in which the agency records are situated, or in the District of Columbia, without regard to the amount in controversy, within two years from the

date on which the cause of action arises, except that where an agency has materially and willfully misrepresented any information required under this section to be disclosed to an individual and the information so misrepresented is material to establishment of the liability of the agency to the individual under this section, the action may be brought at any time within two years after discovery by the individual of the misrepresentation. Nothing in this section shall be construed to authorize any civil action by reason of any injury sustained as the result of a disclosure of a record prior to September 27, 1975.

(h) RIGHTS OF LEGAL GUARDIANS.—For the purposes of this section, the parent of any minor, or the legal guardian of any individual who has been declared to be incompetent due to physical or mental incapacity or age by a court of competent jurisdiction, may act on behalf of the individual.

(i)(1) CRIMINAL PENALTIES.—Any officer or employee of an agency, who by virtue of his employment or official position, has possession of, or access to, agency records which contain individually identifiable information the disclosure of which is prohibited by this section or by rules or regulations established thereunder, and who knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than \$5,000.

(2) Any officer or employee of any agency who willfully maintains a system of records without meeting the notice requirements of subsection (e)(4) of this section shall be guilty of a misdemeanor and fined not more than \$5,000.

(3) Any person who knowingly and willfully requests or obtains any record concerning an individual from an agency under false pretenses shall be guilty of a misdemeanor and fined not more than \$5,000.

(j) GENERAL EXEMPTIONS.—The head of any agency may promulgate rules, in accordance with the requirements (including general notice) of sections 553(b)(1), (2), and (3), (c), and (e) of this title, to exempt any system of records within the agency from any part of this section except subsections (b), (c)(1) and (2), (e)(4)(A) through (F), (e)(6), (7), (9), (10), and (11), and (i) if the system of records is—

(1) maintained by the Central Intelligence Agency; or

(2) maintained by an agency or component thereof which performs as its principal function any activity pertaining to the enforcement of criminal laws, including police efforts to prevent, control, or reduce crime or to apprehend criminals, and the activities of prosecutors, courts, correctional, probation, pardon, or parole authorities, and which consists of (A) information compiled for the purpose of identifying individual

criminal offenders and alleged offenders and consisting only of identifying data and notations of arrests, the nature and disposition of criminal charges, sentencing, confinement, release, and parole and probation status; (B) information compiled for the purpose of a criminal investigation, including reports of informants and investigators, and associated with an identifiable individual; or (C) reports identifiable to an individual compiled at any stage of the process of enforcement of the criminal laws from arrest or indictment through release from supervision.

At the time rules are adopted under this subsection, the agency shall include in the statement required under section 553(c) of this title, the reasons why the system of records is to be exempted from a provision of this section.

(k) SPECIFIC EXEMPTIONS.—The head of any agency may promulgate rules, in accordance with the requirements (including general notice) of sections 553(b)(1), (2), and (3), (c), and (e) of this title, to exempt any system of records within the agency from subsections (c)(3), (d), (e)(1), (e)(4)(G), (H), and (I) and (f) of this section if the system of records is—

- (1) subject to the provisions of section 552(b)(1) of this title;
- (2) investigatory material compiled for law enforcement purposes, other than material within the scope of subsection (j)(2) of this section: Provided, however, That if any individual is denied any right, privilege, or benefit that he would otherwise be entitled by Federal law, or for which he would otherwise be eligible, as a result of the maintenance of such material, such material shall be provided to such individual, except to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the Government under an express promise that the identity of the source would be held in confidence, or, prior to the effective date of this section, under an implied promise that the identity of the source would be held in confidence;
- (3) maintained in connection with providing protective services to the President of the United States or other individuals pursuant to section 3056 of title 18;
- (4) required by statute to be maintained and used solely as statistical records;
- (5) investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment, military service, Federal contracts, or access to classified information, but only to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the Government under an express promise that the identity of the source would be held in confidence, or, prior to the effective date of this section, under an

implied promise that the identity of the source would be held in confidence;

(6) testing or examination material used solely to determine individual qualifications for appointment or promotion in the Federal service the disclosure of which would compromise the objectivity or fairness of the testing or examination process; or

(7) evaluation material used to determine potential for promotion in the armed services, but only to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the Government under an express promise that the identity of the source would be held in confidence, or, prior to the effective date of this section, under an implied promise that the identity of the source would be held in confidence.

At the time rules are adopted under this subsection, the agency shall include in the statement required under section 553(c) of this title, the reasons why the system of records is to be exempted from a provision of this section.

(1)(1) ARCHIVAL RECORDS.—Each agency record which is accepted by the Archivist of the United States for storage, processing, and servicing in accordance with section 3103 of title 44 shall, for the purposes of this section, be considered to be maintained by the agency which deposited the record and shall be subject to the provisions of this section. The Archivist of the United States shall not disclose the record except to the agency which maintains the record, or under rules established by that agency which are not inconsistent with the provisions of this section.

(2) Each agency record pertaining to an identifiable individual which was transferred to the National Archives of the United States as a record which has sufficient historical or other value to warrant its continued preservation by the United States Government, prior to the effective date of this section, shall, for the purposes of this section, be considered to be maintained by the National Archives and shall not be subject to the provisions of this section, except that a statement generally describing such records (modeled after the requirements relating to records subject to subsections (e)(4)(A) through (G) of this section) shall be published in the Federal Register.

(3) Each agency record pertaining to an identifiable individual which is transferred to the National Archives of the United States as a record which has sufficient historical or other value to warrant its continued preservation by the United States Government, on or after the effective date of this section, shall, for the purposes of this section, be considered to be maintained by the National Archives and shall be exempt from the

PRIVACY ACT

requirements of this section except subsections (e)(4)(A) through (G) and (e)(9) of this section.

(m)(1) **GOVERNMENT CONTRACTORS.**—When an agency provides by a contract for the operation by or on behalf of the agency of a system of records to accomplish an agency function, the agency shall, consistent with its authority, cause the requirements of this section to be applied to such system. For purposes of subsection (i) of this section any such contractor and any employee of such contractor, if such contract is agreed to on or after the effective date of this section, shall be considered to be an employee of an agency.

(2) A consumer reporting agency to which a record is disclosed under section 3711(e) of title 31 shall not be considered a contractor for the purposes of this section.

(n) **MAILING LISTS.**—An individual's name and address may not be sold or rented by an agency unless such action is specifically authorized by law. This provision shall not be construed to require the withholding of names and addresses otherwise permitted to be made public.

(o) **MATCHING AGREEMENTS.**—

(1) No record which is contained in a system of records may be disclosed to a recipient agency or non-Federal agency for use in a computer matching program except pursuant to a written agreement between the source agency and the recipient agency or non-Federal agency specifying—

(A) the purpose and legal authority for conducting the program;

(B) the justification for the program and the anticipated results, including a specific estimate of any savings;

(C) a description of the records that will be matched, including each data element that will be used, the approximate number of records that will be matched, and the projected starting and completion dates of the matching program;

(D) procedures for providing individualized notice at the time of application, and notice periodically thereafter as directed by the Data Integrity Board of such agency (subject to guidance provided by the Director of the Office of Management and Budget pursuant to subsection (v)), to—

(i) applicants for and recipients of financial assistance or payments under Federal benefit programs, and

(ii) applicants for and holders of positions as Federal personnel,

that any information provided by such applicants, recipients, holders, and individuals may be subject to verification through matching programs;

- (E) procedures for verifying information produced in such matching program as required by subsection (p);
- (F) procedures for the retention and timely destruction of identifiable records created by a recipient agency or non-Federal agency in such matching program;
- (G) procedures for ensuring the administrative, technical, and physical security of the records matched and the results of such programs;
- (H) prohibitions on duplication and redisclosure of records provided by the source agency within or outside the recipient agency or the non-Federal agency, except where required by law or essential to the conduct of the matching program;
- (I) procedures governing the use by a recipient agency or non-Federal agency of records provided in a matching program by a source agency, including procedures governing return of the records to the source agency or destruction of records used in such program;
- (J) information on assessments that have been made on the accuracy of the records that will be used in such matching program; and
- (K) that the Comptroller General may have access to all records of a recipient agency or a non-Federal agency that the Comptroller General deems necessary in order to monitor or verify compliance with the agreement.

(2)(A) A copy of each agreement entered into pursuant to paragraph (1) shall—

- (i) be transmitted to the Committee on Governmental Affairs of the Senate and the Committee on Government Operations of the House of Representatives; and
- (ii) be available upon request to the public.

(B) No such agreement shall be effective until 30 days after the date on which such a copy is transmitted pursuant to subparagraph (A)(i).

(C) Such an agreement shall remain in effect only for such period, not to exceed 18 months, as the Data Integrity Board of the agency determines is appropriate in light of the purposes, and length of time necessary for the conduct, of the matching program.

(D) Within 3 months prior to the expiration of such an agreement pursuant to subparagraph (C), the Data Integrity Board of the agency may, without additional review, renew the matching

agreement for a current, ongoing matching program for not more than one additional year if—

- (i) such program will be conducted without any change; and
- (ii) each party to the agreement certifies to the Board in writing that the program has been conducted in compliance with the agreement.

(p) VERIFICATION AND OPPORTUNITY TO CONTEST FINDINGS.—

(1) In order to protect any individual whose records are used in a matching program, no recipient agency, non-Federal agency, or source agency may suspend, terminate, reduce, or make a final denial of any financial assistance or payment under a Federal benefit program to such individual, or take other adverse action against such individual, as a result of information produced by such matching program, until—

- (A)(i) the agency has independently verified the information; or
- (ii) the Data Integrity Board of the agency, or in the case of a non-Federal agency the Data Integrity Board of the source agency, determines in accordance with guidance issued by the Director of the Office of Management and Budget that—
 - (I) the information is limited to identification and amount of benefits paid by the source agency under a Federal benefit program; and
 - (II) there is a high degree of confidence that the information provided to the recipient agency is accurate;

(B) the individual receives a notice from the agency containing a statement of its findings and informing the individual of the opportunity to contest such findings; and

(C)(i) the expiration of any time period established for the program by statute or regulation for the individual to respond to that notice; or

- (ii) in the case of a program for which no such period is established, the end of the 30-day period beginning on the date on which notice under subparagraph (B) is mailed or otherwise provided to the individual.

(2) Independent verification referred to in paragraph (1) requires investigation and confirmation of specific information relating to an individual that is used as a basis for an adverse action against the individual, including where applicable investigation and confirmation of—

PRIVACY ACT

- (A) the amount of any asset or income involved;
- (B) whether such individual actually has or had access to such asset or income for such individual's own use; and
- (C) the period or periods when the individual actually had such asset or income.

(3) Notwithstanding paragraph (1), an agency may take any appropriate action otherwise prohibited by such paragraph if the agency determines that the public health or public safety may be adversely affected or significantly threatened during any notice period required by such paragraph.

(q) SANCTIONS.—

(1) Notwithstanding any other provision of law, no source agency may disclose any record which is contained in a system of records to a recipient agency or non-Federal agency for a matching program if such source agency has reason to believe that the requirements of subsection (p), or any matching agreement entered into pursuant to subsection (o), or both, are not being met by such recipient agency.

(2) No source agency may renew a matching agreement unless—

- (A) the recipient agency or non-Federal agency has certified that it has complied with the provisions of that agreement; and
- (B) the source agency has no reason to believe that the certification is inaccurate.

(r) REPORT ON NEW SYSTEMS AND MATCHING PROGRAMS.—Each agency that proposes to establish or make a significant change in a system of records or a matching program shall provide adequate advance notice of any such proposal (in duplicate) to the Committee on Government Operations of the House of Representatives, the Committee on Governmental Affairs of the Senate, and the Office of Management and Budget in order to permit an evaluation of the probable or potential effect of such proposal on the privacy or other rights of individuals.

(s) BIENNIAL REPORT.—The President shall biennially submit to the Speaker of the House of Representatives and the President pro tempore of the Senate a report—

- (1) describing the actions of the Director of the Office of Management and Budget pursuant to section 6 of the Privacy Act of 1974 during the preceding 2 years;
- (2) describing the exercise of individual rights of access and amendment under this section during such years;
- (3) identifying changes in or additions to systems of records;
- (4) containing such other information concerning administration of this section as may be necessary or useful to the Congress in reviewing the

PRIVACY ACT

effectiveness of this section in carrying out the purposes of the Privacy Act of 1974.

(t)(1) EFFECT OF OTHER LAWS.—No agency shall rely on any exemption contained in section 552 of this title to withhold from an individual any record which is otherwise accessible to such individual under the provisions of this section.

(2) No agency shall rely on any exemption in this section to withhold from an individual any record which is otherwise accessible to such individual under the provisions of section 552 of this title.

(u) DATA INTEGRITY BOARDS.—

(1) Every agency conducting or participating in a matching program shall establish a Data Integrity Board to oversee and coordinate among the various components of such agency the agency's implementation of this section.

(2) Each Data Integrity Board shall consist of senior officials designated by the head of the agency, and shall include any senior official designated by the head of the agency as responsible for implementation of this section, and the inspector general of the agency, if any. The inspector general shall not serve as chairman of the Data Integrity Board.

(3) Each Data Integrity Board—

(A) shall review, approve, and maintain all written agreements for receipt or disclosure of agency records for matching programs to ensure compliance with subsection (o), and all relevant statutes, regulations, and guidelines;

(B) shall review all matching programs in which the agency has participated during the year, either as a source agency or recipient agency, determine compliance with applicable laws, regulations, guidelines, and agency agreements, and assess the costs and benefits of such programs;

(C) shall review all recurring matching programs in which the agency has participated during the year, either as a source agency or recipient agency, for continued justification for such disclosures;

(D) shall compile an annual report, which shall be submitted to the head of the agency and the Office of Management and Budget and made available to the public on request, describing the matching activities of the agency, including—

(i) matching programs in which the agency has participated as a source agency or recipient agency;

(ii) matching agreements proposed under subsection (o) that were disapproved by the Board;

- (iii) any changes in membership or structure of the Board in the preceding year;
- (iv) the reasons for any waiver of the requirement in paragraph (4) of this section for completion and submission of a cost-benefit analysis prior to the approval of a matching program;
- (v) any violations of matching agreements that have been alleged or identified and any corrective action taken; and
- (vi) any other information required by the Director of the Office of Management and Budget to be included in such report;

(E) shall serve as a clearinghouse for receiving and providing information on the accuracy, completeness, and reliability of records used in matching programs;

(F) shall provide interpretation and guidance to agency components and personnel on the requirements of this section for matching programs;

(G) shall review agency recordkeeping and disposal policies and practices for matching programs to assure compliance with this section; and

(H) may review and report on any agency matching activities that are not matching programs.

(4)(A) Except as provided in subparagraphs (B) and (C), a Data Integrity Board shall not approve any written agreement for a matching program unless the agency has completed and submitted to such Board a cost-benefit analysis of the proposed program and such analysis demonstrates that the program is likely to be cost effective.

(B) The Board may waive the requirements of subparagraph (A) of this paragraph if it determines in writing, in accordance with guidelines prescribed by the Director of the Office of Management and Budget, that a cost-benefit analysis is not required.

(C) A cost-benefit analysis shall not be required under subparagraph (A) prior to the initial approval of a written agreement for a matching program that is specifically required by statute. Any subsequent written agreement for such a program shall not be approved by the Data Integrity Board unless the agency has submitted a cost-benefit analysis of the program as conducted under the preceding approval of such agreement.

PRIVACY ACT

(5)(A) If a matching agreement is disapproved by a Data Integrity Board, any party to such agreement may appeal the disapproval to the Director of the Office of Management and Budget. Timely notice of the filing of such an appeal shall be provided by the Director of the Office of Management and Budget to the Committee on Governmental Affairs of the Senate and the Committee on Government Operations of the House of Representatives.

(B) The Director of the Office of Management and Budget may approve a matching agreement notwithstanding the disapproval of a Data Integrity Board if the Director determines that—

- (i) the matching program will be consistent with all applicable legal, regulatory, and policy requirements;
- (ii) there is adequate evidence that the matching agreement will be cost-effective; and
- (iii) the matching program is in the public interest.

(C) The decision of the Director to approve a matching agreement shall not take effect until 30 days after it is reported to committees described in subparagraph (A).

(D) If the Data Integrity Board and the Director of the Office of Management and Budget disapprove a matching program proposed by the inspector general of an agency, the inspector general may report the disapproval to the head of the agency and to the Congress.

(6) In the reports required by paragraph (3)(D), agency matching activities that are not matching programs may be reported on an aggregate basis, if and to the extent necessary to protect ongoing law enforcement or counterintelligence investigations.

(v) OFFICE OF MANAGEMENT AND BUDGET RESPONSIBILITIES.—The Director of the Office of Management and Budget shall—

- (1) develop and, after notice and opportunity for public comment, prescribe guidelines and regulations for the use of agencies in implementing the provisions of this section; and
- (2) provide continuing assistance to and oversight of the implementation of this section by agencies.

(w) APPLICABILITY TO BUREAU OF CONSUMER FINANCIAL PROTECTION.—Except as provided in the Consumer Financial Protection Act of 2010, this section shall apply with respect to the Bureau of Consumer Financial Protection.

WAR CRIMES ACT OF 1996

[Public Law 104-192; 110 Stat. 2104; August 21, 1996]

AN ACT to amend title 18, United States Code, to carry out the international obligations of the United States under the Geneva Conventions to provide criminal penalties for certain war crimes.

Be it enacted by the Senate and House of Representatives for the United States of America in Congress assembled,

SHORT TITLE

SEC. 1. This Act may be cited as the “War Crimes Act of 1996”.

CRIMINAL PENALTIES FOR CERTAIN WAR CRIMES

SEC. 2. [Amending 18 U.S.C. § 2441 to read as follows:]

WAR CRIMES

SEC. 2441.¹

(a) **OFFENSE.**—Whoever, whether inside or outside the United States, commits a war crime, in any of the circumstances described in subsection (b), shall be fined under this title or imprisoned for life or any term of years, or both, and if death results to the victim, shall also be subject to the penalty of death.

(b) **JURISDICTION.**—There is jurisdiction over an offense described in subsection (a) if—

(1) the offense occurs in whole or in part within the United States; or

(2) regardless of where the offense occurs—

(A) the victim or offender is—

(i) a national of the United States or an alien lawfully admitted for permanent resident; or

(ii) a member of the Armed Forces of the United States, regardless of nationality; or

(B) the offender is present in the United States, regardless of the nationality of the victim or offender.

¹ Including amendments to 18 U.S.C. § 2441 made by other Acts.

(c) DEFINITION.—As used in this section the term “war crime” means any conduct—

- (1) defined as a grave breach in any of the international conventions signed at Geneva 12 August 1949, or any protocol to such convention to which the United States is a party;
- (2) prohibited by Article 23, 25, 27, or 28 of the Annex to the Hague Convention IV, Respecting the Laws and Customs of War on Land, signed 18 October 1907;
- (3) which constitutes a grave breach of common Article 3 (as defined in subsection (d)) when committed in the context of and in association with an armed conflict not of an international character; or
- (4) of a person who, in relation to an armed conflict and contrary to the provisions of the Protocol on Prohibitions or Restrictions on the Use of Mines, Booby-Traps and Other Devices as amended at Geneva on 3 May 1996 (Protocol II as amended on 3 May 1996), when the United States is a party to such Protocol, willfully kills or causes serious injury to civilians.

(d) COMMON ARTICLE 3 VIOLATIONS.—

(1) PROHIBITED CONDUCT.—In subsection (c)(3), the term “grave breach of common Article 3” means any conduct (such conduct constituting a grave breach of common Article 3 of the international conventions done at Geneva August 12, 1949), as follows:

- (A) TORTURE.—The act of a person who commits, or conspires or attempts to commit, an act specifically intended to inflict severe physical or mental pain or suffering (other than pain or suffering incidental to lawful sanctions) upon another person within his custody or physical control for the purpose of obtaining information or a confession, punishment, intimidation, coercion, or any reason based on discrimination of any kind.
- (B) CRUEL OR INHUMAN TREATMENT.—The act of a person who commits, or conspires or attempts to commit, an act intended to inflict severe or serious physical or mental pain or suffering (other than pain or suffering incidental to lawful sanctions), including serious physical abuse, upon another within his custody or control.
- (C) PERFORMING BIOLOGICAL EXPERIMENTS.—The act of a person who subjects, or conspires or attempts to subject, one or more persons within his custody or physical control to biological experiments without a legitimate medical or dental purpose and in so doing endangers the body or health of such person or persons.

(D) MURDER.—The act of a person who intentionally kills, or conspires or attempts to kill, or kills whether intentionally or unintentionally in the course of committing any other offense under this subsection, one or more persons taking no active part in the hostilities, including those placed out of combat by sickness, wounds, detention, or any other cause.

(E) MUTILATION OR MAIMING.—The act of a person who intentionally injures, or conspires or attempts to injure, or injures whether intentionally or unintentionally in the course of committing any other offense under this subsection, one or more persons taking no active part in the hostilities, including those placed out of combat by sickness, wounds, detention, or any other cause, by disfiguring the person or persons by any mutilation thereof or by permanently disabling any member, limb, or organ of his body, without any legitimate medical or dental purpose.

(F) INTENTIONALLY CAUSING SERIOUS BODILY INJURY.—The act of a person who intentionally causes, or conspires or attempts to cause, serious bodily injury to one or more persons, including lawful combatants, in violation of the law of war.

(G) RAPE.—The act of a person who forcibly or with coercion or threat of force wrongfully invades, or conspires or attempts to invade, the body of a person by penetrating, however slightly, the anal or genital opening of the victim with any part of the body of the accused, or with any foreign object.

(H) SEXUAL ASSAULT OR ABUSE.—The act of a person who forcibly or with coercion or threat of force engages, or conspires or attempts to engage, in sexual contact with one or more persons, or causes, or conspires or attempts to cause, one or more persons to engage in sexual contact.

(I) TAKING HOSTAGES.—The act of a person who, having knowingly seized or detained one or more persons, threatens to kill, injure, or continue to detain such person or persons with the intent of compelling any nation, person other than the hostage, or group of persons to act or refrain from acting as an explicit or implicit condition for the safety or release of such person or persons.

(2) DEFINITIONS.—In the case of an offense under subsection (a) by reason of subsection (c)(3)—

(A) the term “severe mental pain or suffering” shall be applied for purposes of paragraphs (1)(A) and (1)(B) in accordance with the meaning given that term in section 2340(2) of this title;

(B) the term “serious bodily injury” shall be applied for purposes of paragraph (1)(F) in accordance with the meaning given that term in section 113(b)(2) of this title;

(C) the term “sexual contact” shall be applied for purposes of paragraph (1)(G) in accordance with the meaning given that term in section 2246(3) of this title;

(D) the term “serious physical pain or suffering” shall be applied for purposes of paragraph (1)(B) as meaning bodily injury that involves—

- (i) a substantial risk of death;
- (ii) extreme physical pain;
- (iii) a burn or physical disfigurement of a serious nature (other than cuts, abrasions, or bruises); or
- (iv) significant loss or impairment of the function of a bodily member, organ, or mental faculty; and

(E) the term “serious mental pain or suffering” shall be applied for purposes of paragraph (1)(B) in accordance with the meaning given the term “severe mental pain or suffering” (as defined in section 2340(2) of this title), except that—

- (i) the term “serious” shall replace the term “severe” where it appears; and
- (ii) as to conduct occurring after the date of the enactment of the Military Commissions Act of 2006, the term “serious and non-transitory mental harm (which need not be prolonged)” shall replace the term “prolonged mental harm” where it appears.

(3) **INAPPLICABILITY OF CERTAIN PROVISIONS WITH RESPECT TO COLLATERAL DAMAGE OR INCIDENT OF LAWFUL ATTACK.**—The intent specified for the conduct stated in subparagraphs (D), (E), and (F) or paragraph (1) precludes the applicability of those subparagraphs to an offense under subsection (a) by reasons of subsection (c)(3) with respect to—

- (A) collateral damage; or
- (B) death, damage, or injury incident to a lawful attack.

(4) **INAPPLICABILITY OF TAKING HOSTAGES TO PRISONER EXCHANGE.**—Paragraph (1)(I) does not apply to an offense under subsection (a) by reason of subsection (c)(3) in the case of a prisoner exchange during wartime.

(5) DEFINITION OF GRAVE BREACHES.—The definitions in this subsection are intended only to define the grave breaches of common Article 3 and not the full scope of United States obligations under that Article.

(e) NONAPPLICABILITY OF CERTAIN LIMITATIONS.—In the case of an offense described in subsection (a) and further described in subsections (c)(1) and (c)(3), an indictment may be found or an information may be instituted at any time without limitation.

(f) CERTIFICATION REQUIREMENT.—

(1) IN GENERAL.—No prosecution for an offense described in subsection (a) shall be undertaken by the United States except on written certification of the Attorney General, the Deputy Attorney General, or an Assistant Attorney General, which function of approving prosecutions may not be delegated, that a prosecution by the United States is in the public interest and necessary to secure substantial justice.

(2) OFFENDER PRESENT IN UNITED STATES.—For an offense for which jurisdiction exists under subsection (b)(2)(B) (and does not exist under any other provision of subsection (b)), the written certification required under paragraph (1) of this subsection that a prosecution by the United States is in the public interest and necessary to secure substantial justice shall be made by the Attorney General or the Deputy Attorney General, which function may not be delegated. In issuing such certification, the same official shall weigh and consider, among other relevant factors—

(A) whether the alleged offender can be removed from the United State for purposes of prosecution in another jurisdiction; and

(B) potential adverse consequences for nationals, servicemembers, or employees of the United States.

(g) INPUT FROM OTHER AGENCY HEADS.—The Secretary of Defense and Secretary of State may submit to the Attorney General for consideration their views generally regarding potential benefits, or potential adverse consequences for nationals, servicemembers, or employees of the United States, of prosecutions of offenses for which jurisdiction exists under subsection (b)(2)(B).

(h) NO JUDICIAL REVIEW.—Certifications under subsection (f) and input from other agency heads under subsection (g) are not subject to judicial review.

(i) RULES OF CONSTRUCTION.—Nothing in this section shall be construed as—

(1) support for ratification of or accession to the Rome Statute of the International Criminal Court, which entered into force on July 1, 2002;
or

(2) consent by the United States to any assertion or exercise of jurisdiction by any international, hybrid, or foreign court.

**INTERCEPTION AND DISCLOSURE OF WIRE, ORAL OR
ELECTRONIC COMMUNICATIONS PROHIBITED**

CHAPTER 119 OF TITLE 18, UNITED STATES CODE

SEC. 2511.

- (1) Except as otherwise specifically provided in this chapter any person who—
- (a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication;
 - (b) intentionally uses, endeavors to use, or procures any other person to use or endeavor to use any electronic, mechanical, or other device to intercept any oral communication when—
 - (i) such device is affixed to, or otherwise transmits a signal through, a wire, cable, or other like connection used in wire communication; or
 - (ii) such device transmits communications by radio, or interferes with the transmission of such communication; or
 - (iii) such person knows, or has reason to know, that such device or any component thereof has been sent through the mail or transported in interstate or foreign commerce; or
 - (iv) such use or endeavor to use (A) takes place on the premises of any business or other commercial establishment the operations of which affect interstate or foreign commerce; or (B) obtains or is for the purpose of obtaining information relating to the operations of any business or other commercial establishment the operations of which affect interstate or foreign commerce; or
 - (v) such person acts in the District of Columbia, the Commonwealth of Puerto Rico, or any territory or possession of the United States;
 - (c) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection;
 - (d) intentionally uses, or endeavors to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection; or
 - (e)(i) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication,

intercepted by means authorized by sections 2511(2)(a)(ii), 2511(2)(b)-(c), 2511(2)(e), 2516, and 2518 of this chapter,

(ii) knowing or having reason to know that the information was obtained through the interception of such a communication in connection with a criminal investigation,

(iii) having obtained or received the information in connection with a criminal investigation, and

(iv) with intent to improperly obstruct, impede, or interfere with a duly authorized criminal investigation,

shall be punished as provided in subsection (4) or shall be subject to suit as provided in subsection (5).

(2)(a)(i) It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks.

(ii) Notwithstanding any other law, providers of wire or electronic communication service, their officers, employees, and agents, landlords, custodians, or other persons, are authorized to provide information, facilities, or technical assistance to persons authorized by law to intercept wire, oral, or electronic communications or to conduct electronic surveillance, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, if such provider, its officers, employees, or agents, landlord, custodian, or other specified person, has been provided with—

(A) a court order directing such assistance or a court order pursuant to section 704 of the Foreign Intelligence Surveillance Act of 1978 signed by the authorizing judge, or

(B) a certification in writing by a person specified in section 2518(7) of this title or the Attorney General of the United States that no warrant or court order is required by law, that all statutory requirements have been met, and that the specified assistance is required, setting forth the period of time during which the provision of the information, facilities, or technical assistance is authorized and

specifying the information, facilities, or technical assistance required. No provider of wire or electronic communication service, officer, employee, or agent thereof, or landlord, custodian, or other specified person shall disclose the existence of any interception or surveillance or the device used to accomplish the interception or surveillance with respect to which the person has been furnished a court order or certification under this chapter, except as may otherwise be required by legal process and then only after prior notification to the Attorney General or to the principal prosecuting attorney of a State or any political subdivision of a State, as may be appropriate. Any such disclosure, shall render such person liable for the civil damages provided for in section 2520. No cause of action shall lie in any court against any provider of wire or electronic communication service, its officers, employees, or agents, landlord, custodian, or other specified person for providing information, facilities, or assistance in accordance with the terms of a court order, statutory authorization, or certification under this chapter.

(iii) If a certification under subparagraph (ii)(B) for assistance to obtain foreign intelligence information is based on statutory authority, the certification shall identify the specific statutory provision and shall certify that the statutory requirements have been met.

(b) It shall not be unlawful under this chapter for an officer, employee, or agent of the Federal Communications Commission, in the normal course of his employment and in discharge of the monitoring responsibilities exercised by the Commission in the enforcement of chapter 5 of title 47 of the United States Code, to intercept a wire or electronic communication, or oral communication transmitted by radio, or to disclose or use the information thereby obtained.

(c) It shall not be unlawful under this chapter for a person acting under color of law to intercept a wire, oral, or electronic communication, where such person is a party to the communication or one of the parties to the communication has given prior consent to such interception.

(d) It shall not be unlawful under this chapter for a person not acting under color of law to intercept a wire, oral, or electronic communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State.

(e) Notwithstanding any other provision of this title or section 705 or 706 of the Communications Act of 1934, it shall not be unlawful for an officer, employee, or agent of the United States in the normal course of his official duty to conduct electronic surveillance, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, as authorized by that Act.

(f) Nothing contained in this chapter or chapter 121 or 206 of this title, or section 705 of the Communications Act of 1934, shall be deemed to affect the acquisition by the United States Government of foreign intelligence information from international or foreign communications, or foreign intelligence activities conducted in accordance with otherwise applicable Federal law involving a foreign electronic communications system, utilizing a means other than electronic surveillance as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, and procedures in this chapter or chapter 121 and the Foreign Intelligence Surveillance Act of 1978 shall be the exclusive means by which electronic surveillance, as defined in section 101 of such Act, and the interception of domestic wire, oral, and electronic communications may be conducted.

(g) It shall not be unlawful under this chapter or chapter 121 of this title for any person—

(i) to intercept or access an electronic communication made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public;

(ii) to intercept any radio communication which is transmitted—

(I) by any station for the use of the general public, or that relates to ships, aircraft, vehicles, or persons in distress;

(II) by any governmental, law enforcement, civil defense, private land mobile, or public safety communications system, including police and fire, readily accessible to the general public;

(III) by a station operating on an authorized frequency within the bands allocated to the amateur, citizens band, or general mobile radio services; or

(IV) by any marine or aeronautical communications system;

(iii) to engage in any conduct which—

(I) is prohibited by section 633 of the Communications Act of 1934; or

- (II) is excepted from the application of section 705(a) of the Communications Act of 1934 by section 705(b) of that Act;
 - (iv) to intercept any wire or electronic communication the transmission of which is causing harmful interference to any lawfully operating station or consumer electronic equipment, to the extent necessary to identify the source of such interference; or
 - (v) for other users of the same frequency to intercept any radio communication made through a system that utilizes frequencies monitored by individuals engaged in the provision or the use of such system, if such communication is not scrambled or encrypted.
- (h) It shall not be unlawful under this chapter—
- (i) to use a pen register or a trap and trace device (as those terms are defined for the purposes of chapter 206 (relating to pen registers and trap and trace devices) of this title); or
 - (ii) for a provider of electronic communication service to record the fact that a wire or electronic communication was initiated or completed in order to protect such provider, another provider furnishing service toward the completion of the wire or electronic communication, or a user of that service, from fraudulent, unlawful or abusive use of such service.
- (i) It shall not be unlawful under this chapter for a person acting under color of law to intercept the wire or electronic communications of a computer trespasser transmitted to, through, or from the protected computer, if—
- (I) the owner or operator of the protected computer authorizes the interception of the computer trespasser's communications on the protected computer;
 - (II) the person acting under color of law is lawfully engaged in an investigation;
 - (III) the person acting under color of law has reasonable grounds to believe that the contents of the computer trespasser's communications will be relevant to the investigation; and
 - (IV) such interception does not acquire communications other than those transmitted to or from the computer trespasser.
- (j) It shall not be unlawful under this chapter for a provider of electronic communication service to the public or remote computing service to intercept or disclose the contents of a wire or electronic communication in response to an order from a foreign government that is subject to an

executive agreement that the Attorney General has determined and certified to Congress satisfies section 2523.

(3)(a) Except as provided in paragraph (b) of this subsection, a person or entity providing an electronic communication service to the public shall not intentionally divulge the contents of any communication (other than one to such person or entity, or an agent thereof) while in transmission on that service to any person or entity other than an addressee or intended recipient of such communication or an agent of such addressee or intended recipient.

(b) A person or entity providing electronic communication service to the public may divulge the contents of any such communication—

- (i) as otherwise authorized in section 2511(2)(a) or 2517 of this title;
- (ii) with the lawful consent of the originator or any addressee or intended recipient of such communication;
- (iii) to a person employed or authorized, or whose facilities are used, to forward such communication to its destination; or
- (iv) which were inadvertently obtained by the service provider and which appear to pertain to the commission of a crime, if such divulgence is made to a law enforcement agency.

(4)(a) Except as provided in paragraph (b) of this subsection or in subsection (5), whoever violates subsection (1) of this section shall be fined under this title or imprisoned not more than five years, or both.

(b) Conduct otherwise an offense under this subsection that consists of or relates to the interception of a satellite transmission that is not encrypted or scrambled and that is transmitted—

- (i) to a broadcasting station for purposes of retransmission to the general public; or
- (ii) as an audio subcarrier intended for redistribution to facilities open to the public, but not including data transmissions or telephone calls,

is not an offense under this subsection unless the conduct is for the purposes of direct or indirect commercial advantage or private financial gain.

(5)(a)(i) If the communication is—

(A) a private satellite video communication that is not scrambled or encrypted and the conduct in violation of this chapter is the private viewing of that communication and is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain; or

(B) a radio communication that is transmitted on frequencies allocated under subpart D of part 74 of the rules of the Federal Communications Commission that is not scrambled or encrypted and the conduct in violation of this chapter is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain,

then the person who engages in such conduct shall be subject to suit by the Federal Government in a court of competent jurisdiction.

(ii) In an action under this subsection—

(A) if the violation of this chapter is a first offense for the person under paragraph (a) of subsection (4) and such person has not been found liable in a civil action under section 2520 of this title, the Federal Government shall be entitled to appropriate injunctive relief; and
(B) if the violation of this chapter is a second or subsequent offense under paragraph (a) of subsection (4) or such person has been found liable in any prior civil action under section 2520, the person shall be subject to a mandatory \$500 civil fine.

(b) The court may use any means within its authority to enforce an injunction issued under paragraph (ii)(A), and shall impose a civil fine of not less than \$500 for each violation of such an injunction.

EXECUTIVE ORDER 12139, FOREIGN INTELLIGENCE ELECTRONIC
SURVEILLANCE

EXECUTIVE ORDER 12139:
FOREIGN INTELLIGENCE ELECTRONIC SURVEILLANCE

[Signed: May 23, 1979, Federal Register Vol. 44, No. 103 (May 25, 1979), as amended by EO 12333 (1981), EO 13383 (2005), and EO 13475 (2008)]

By the authority vested in me as President by Sections 102 and 104 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1802 and 1804), in order to provide as set forth in that Act for the authorization of electronic surveillance for foreign intelligence purposes, it is hereby ordered as follows:

1-101. Pursuant to Section 102(a)(1) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1802(a)), the Attorney General is authorized to approve electronic surveillance to acquire foreign intelligence information without a court order, but only if the Attorney General makes the certifications required by that Section.

1-102. Pursuant to Section 102(b) of the Foreign Intelligence Act of 1978 (50 U.S.C. 1802(b)), the Attorney General is authorized to approve applications to the court having jurisdiction under Section 103 of that Act (50 U.S.C. 1803) to obtain orders for electronic surveillance for the purpose of obtaining foreign intelligence information.

1-103. Pursuant to Section 104(a)(6) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1804(a)(6)), the following officials, each of whom is employed in the area of national security or defense, is designated to make the certifications required by Section 104(a)(6) of the Act in support of applications to conduct electronic surveillance:

- (a) Secretary of State.
- (b) Secretary of Defense.
- (c) Director of National Intelligence.
- (d) Director of the Federal Bureau of Investigation.
- (e) Deputy Secretary of State.
- (f) Deputy Secretary of Defense.
- (g) Director of the Central Intelligence Agency.
- (h) Principal Deputy Director of National Intelligence; and
- (i) Deputy Director of the Federal Bureau of Investigation.

EXECUTIVE ORDER 12139, FOREIGN INTELLIGENCE ELECTRONIC
SURVEILLANCE

None of the above officials, nor anyone officially acting in that capacity, may exercise the authority to make the above certifications, unless that official has been appointed by the President with the advice and consent of the Senate. The requirement of the preceding sentence that the named official must be appointed by the President with the advice and consent of the Senate does not apply to the Deputy Director of the Federal Bureau of Investigation.

[Sections 1-104 and 1-105 amended EO 12036 which was revoked by EO 12333.]

-/S/- Jimmy Carter.
THE WHITE HOUSE,
May 23, 1979.

EXECUTIVE ORDER 12333:
UNITED STATES INTELLIGENCE ACTIVITIES

[Signed: December 4, 1981, Federal Register Vol. 46, No. 235 (December 8, 1981), as amended by EO 13284 (2003), EO 13355 (2004), and EO 13470 (2008)]

PREAMBLE

Timely, accurate, and insightful information about the activities, capabilities, plans, and intentions of foreign powers, organizations, and persons, and their agents, is essential to the national security of the United States. All reasonable and lawful means must be used to ensure that the United States will receive the best intelligence possible. For that purpose, by virtue of the authority vested in me by the Constitution and the laws of the United States of America, including the National Security Act of 1947, as amended, (Act) and as President of the United States of America, in order to provide for the effective conduct of United States intelligence activities and the protection of constitutional rights, it is hereby ordered as follows:

**PART 1 – GOALS, DIRECTIONS, DUTIES, AND RESPONSIBILITIES
WITH RESPECT TO UNITED STATES INTELLIGENCE EFFORTS**

SECTION 1.1 GOALS. The United States intelligence effort shall provide the President, the National Security Council, and the Homeland Security Council with the necessary information on which to base decisions concerning the development and conduct of foreign, defense, and economic policies, and the protection of United States national interests from foreign security threats. All departments and agencies shall cooperate fully to fulfill this goal.

- (a) All means, consistent with applicable Federal law and this order, and with full consideration of the rights of United States persons, shall be used to obtain reliable intelligence information to protect the United States and its interests.
- (b) The United States Government has a solemn obligation, and shall continue in the conduct of intelligence activities under this order, to protect fully the legal rights of all United States persons, including freedoms, civil liberties, and privacy rights guaranteed by Federal law.
- (c) Intelligence collection under this order should be guided by the need for information to respond to intelligence priorities set by the President.
- (d) Special emphasis should be given to detecting and countering:
 - (1) Espionage and other threats and activities directed by foreign powers or their intelligence services against the United States and its interests;

- (2) Threats to the United States and its interests from terrorism; and
- (3) Threats to the United States and its interests from the development, possession, proliferation, or use of weapons of mass destruction.

(e) Special emphasis shall be given to the production of timely, accurate, and insightful reports, responsive to decisionmakers in the executive branch, that draw on all appropriate sources of information, including open source information, meet rigorous analytic standards, consider diverse analytic viewpoints, and accurately represent appropriate alternative views.

(f) State, local, and tribal governments are critical partners in securing and defending the United States from terrorism and other threats to the United States and its interests. Our national intelligence effort should take into account the responsibilities and requirements of State, local, and tribal governments and, as appropriate, private sector entities, when undertaking the collection and dissemination of information and intelligence to protect the United States.

(g) All departments and agencies have a responsibility to prepare and to provide intelligence in a manner that allows the full and free exchange of information, consistent with applicable law and presidential guidance.

SEC. 1.2 THE NATIONAL SECURITY COUNCIL.

(a) **PURPOSE.** The National Security Council (NSC) shall act as the highest ranking executive branch entity that provides support to the President for review of, guidance for, and direction to the conduct of all foreign intelligence, counterintelligence, and covert action, and attendant policies and programs.

(b) **COVERT ACTION AND OTHER SENSITIVE INTELLIGENCE OPERATIONS.** The NSC shall consider and submit to the President a policy recommendation, including all dissents, on each proposed covert action and conduct a periodic review of ongoing covert action activities, including an evaluation of the effectiveness and consistency with current national policy of such activities and consistency with applicable legal requirements. The NSC shall perform such other functions related to covert action as the President may direct, but shall not undertake the conduct of covert actions. The NSC shall also review proposals for other sensitive intelligence operations.

SEC. 1.3 DIRECTOR OF NATIONAL INTELLIGENCE. Subject to the authority, direction, and control of the President, the Director of National Intelligence (Director) shall serve as the head of the Intelligence Community, act as the principal adviser to the President, to the NSC, and to the Homeland Security Council for intelligence matters related to national security, and shall oversee and direct the implementation of the National Intelligence Program and execution of the National Intelligence Program budget. The Director will lead a unified, coordinated, and effective intelligence effort. In addition, the Director shall, in

carrying out the duties and responsibilities under this section, take into account the views of the heads of departments containing an element of the Intelligence Community and of the Director of the Central Intelligence Agency.

(a) Except as otherwise directed by the President or prohibited by law, the Director shall have access to all information and intelligence described in section 1.5(a) of this order. For the purpose of access to and sharing of information and intelligence, the Director:

- (1) Is hereby assigned the function under section 3(5) of the Act, to determine that intelligence, regardless of the source from which derived and including information gathered within or outside the United States, pertains to more than one United States Government agency; and
- (2) Shall develop guidelines for how information or intelligence is provided to or accessed by the Intelligence Community in accordance with section 1.5(a) of this order, and for how the information or intelligence may be used and shared by the Intelligence Community. All guidelines developed in accordance with this section shall be approved by the Attorney General and, where applicable, shall be consistent with guidelines issued pursuant to section 1016 of the Intelligence Reform and Terrorism Protection Act of 2004 (Public Law 108-458) (IRTPA).

(b) In addition to fulfilling the obligations and responsibilities prescribed by the Act, the Director:

- (1) Shall establish objectives, priorities, and guidance for the Intelligence Community to ensure timely and effective collection, processing, analysis, and dissemination of intelligence, of whatever nature and from whatever source derived;
- (2) May designate, in consultation with affected heads of departments or Intelligence Community elements, one or more Intelligence Community elements to develop and to maintain services of common concern on behalf of the Intelligence Community if the Director determines such services can be more efficiently or effectively accomplished in a consolidated manner;
- (3) Shall oversee and provide advice to the President and the NSC with respect to all ongoing and proposed covert action programs;
- (4) In regard to the establishment and conduct of intelligence arrangements and agreements with foreign governments and international organizations:
 - (A) May enter into intelligence and counterintelligence arrangements and agreements with foreign governments and international organizations;

- (B) Shall formulate policies concerning intelligence and counterintelligence arrangements and agreements with foreign governments and international organizations; and
- (C) Shall align and synchronize intelligence and counterintelligence foreign relationships among the elements of the Intelligence Community to further United States national security, policy, and intelligence objectives;
- (5) Shall participate in the development of procedures approved by the Attorney General governing criminal drug intelligence activities abroad to ensure that these activities are consistent with foreign intelligence programs;
- (6) Shall establish common security and access standards for managing and handling intelligence systems, information, and products, with special emphasis on facilitating:
 - (A) The fullest and most prompt access to and dissemination of information and intelligence practicable, assigning the highest priority to detecting, preventing, preempting, and disrupting terrorist threats and activities against the United States, its interests, and allies; and
 - (B) The establishment of standards for an interoperable information sharing enterprise that facilitates the sharing of intelligence information among elements of the Intelligence Community;
- (7) Shall ensure that appropriate departments and agencies have access to intelligence and receive the support needed to perform independent analysis;
- (8) Shall protect, and ensure that programs are developed to protect, intelligence sources, methods, and activities from unauthorized disclosure;
- (9) Shall, after consultation with the heads of affected departments and agencies, establish guidelines for Intelligence Community elements for:
 - (A) Classification and declassification of all intelligence and intelligence-related information classified under the authority of the Director or the authority of the head of a department or Intelligence Community element; and
 - (B) Access to and dissemination of all intelligence and intelligence-related information, both in its final form and in the form when initially gathered, to include intelligence originally classified by the head of a department or Intelligence Community element, except that access to and dissemination of

- information concerning United States persons shall be governed by procedures developed in accordance with Part 2 of this order;
- (10) May, only with respect to Intelligence Community elements, and after consultation with the head of the originating Intelligence Community element or the head of the originating department, declassify, or direct the declassification of, information or intelligence relating to intelligence sources, methods, and activities. The Director may only delegate this authority to the Principal Deputy Director of National Intelligence;
- (11) May establish, operate, and direct one or more national intelligence centers to address intelligence priorities;
- (12) May establish Functional Managers and Mission Managers, and designate officers or employees of the United States to serve in these positions.

(A) Functional Managers shall report to the Director concerning the execution of their duties as Functional Managers, and may be charged with developing and implementing strategic guidance, policies, and procedures for activities related to a specific intelligence discipline or set of intelligence activities; set training and tradecraft standards; and ensure coordination within and across intelligence disciplines and Intelligence Community elements and with related non-intelligence activities. Functional Managers may also advise the Director on: the management of resources; policies and procedures; collection capabilities and gaps; processing and dissemination of intelligence; technical architectures; and other issues or activities determined by the Director.

(i) The Director of the National Security Agency is designated the Functional Manager for signals intelligence;

(ii) The Director of the Central Intelligence Agency is designated the Functional Manager for human intelligence; and

(iii) The Director of the National Geospatial-Intelligence Agency is designated the Functional Manager for geospatial intelligence.

- (B) Mission Managers shall serve as principal substantive advisors on all or specified aspects of intelligence related to designated countries, regions, topics, or functional issues;
- (13) Shall establish uniform criteria for the determination of relative priorities for the transmission of critical foreign intelligence, and advise

the Secretary of Defense concerning the communications requirements of the Intelligence Community for the transmission of such communications;

(14) Shall have ultimate responsibility for production and dissemination of intelligence produced by the Intelligence Community and authority to levy analytic tasks on intelligence production organizations within the Intelligence Community, in consultation with the heads of the Intelligence Community elements concerned;

(15) May establish advisory groups for the purpose of obtaining advice from within the Intelligence Community to carry out the Director's responsibilities, to include Intelligence Community executive management committees composed of senior Intelligence Community leaders. Advisory groups shall consist of representatives from elements of the Intelligence Community, as designated by the Director, or other executive branch departments, agencies, and offices, as appropriate;

(16) Shall ensure the timely exploitation and dissemination of data gathered by national intelligence collection means, and ensure that the resulting intelligence is disseminated immediately to appropriate government elements, including military commands;

(17) Shall determine requirements and priorities for, and manage and direct the tasking, collection, analysis, production, and dissemination of, national intelligence by elements of the Intelligence Community, including approving requirements for collection and analysis and resolving conflicts in collection requirements and in the tasking of national collection assets of Intelligence Community elements (except when otherwise directed by the President or when the Secretary of Defense exercises collection tasking authority under plans and arrangements approved by the Secretary of Defense and the Director);

(18) May provide advisory tasking concerning collection and analysis of information or intelligence relevant to national intelligence or national security to departments, agencies, and establishments of the United States Government that are not elements of the Intelligence Community; and shall establish procedures, in consultation with affected heads of departments or agencies and subject to approval by the Attorney General, to implement this authority and to monitor or evaluate the responsiveness of United States Government departments, agencies, and other establishments;

(19) Shall fulfill the responsibilities in section 1.3(b)(17) and (18) of this order, consistent with applicable law and with full consideration of the rights of United States persons, whether information is to be collected inside or outside the United States;

(20) Shall ensure, through appropriate policies and procedures, the deconfliction, coordination, and integration of all intelligence activities conducted by an Intelligence Community element or funded by the National Intelligence Program. In accordance with these policies and procedures:

(A) The Director of the Federal Bureau of Investigation shall coordinate the clandestine collection of foreign intelligence collected through human sources or through human-enabled means and counterintelligence activities inside the United States;

(B) The Director of the Central Intelligence Agency shall coordinate the clandestine collection of foreign intelligence collected through human sources or through human-enabled means and counterintelligence activities outside the United States;

(C) All policies and procedures for the coordination of counterintelligence activities and the clandestine collection of foreign intelligence inside the United States shall be subject to the approval of the Attorney General; and

(D) All policies and procedures developed under this section shall be coordinated with the heads of affected departments and Intelligence Community elements;

(21) Shall, with the concurrence of the heads of affected departments and agencies, establish joint procedures to deconflict, coordinate, and synchronize intelligence activities conducted by an Intelligence Community element or funded by the National Intelligence Program, with intelligence activities, activities that involve foreign intelligence and security services, or activities that involve the use of clandestine methods, conducted by other United States Government departments, agencies, and establishments;

(22) Shall, in coordination with the heads of departments containing elements of the Intelligence Community, develop procedures to govern major system acquisitions funded in whole or in majority part by the National Intelligence Program;

(23) Shall seek advice from the Secretary of State to ensure that the foreign policy implications of proposed intelligence activities are considered, and shall ensure, through appropriate policies and procedures, that intelligence activities are conducted in a manner consistent with the responsibilities pursuant to law and presidential direction of Chiefs of United States Missions; and

(24) Shall facilitate the use of Intelligence Community products by the Congress in a secure manner.

(c) The Director's exercise of authorities in the Act and this order shall not abrogate the statutory or other responsibilities of the heads of departments of the United States Government or the Director of the Central Intelligence Agency. Directives issued and actions taken by the Director in the exercise of the Director's authorities and responsibilities to integrate, coordinate, and make the Intelligence Community more effective in providing intelligence related to national security shall be implemented by the elements of the Intelligence Community, provided that any department head whose department contains an element of the Intelligence Community and who believes that a directive or action of the Director violates the requirements of section 1018 of the IRTPA or this subsection shall bring the issue to the attention of the Director, the NSC, or the President for resolution in a manner that respects and does not abrogate the statutory responsibilities of the heads of the departments.

(d) APPOINTMENTS TO CERTAIN POSITIONS.

(1) The relevant department or bureau head shall provide recommendations and obtain the concurrence of the Director for the selection of: the Director of the National Security Agency, the Director of the National Reconnaissance Office, the Director of the National Geospatial-Intelligence Agency, the Under Secretary of Homeland Security for Intelligence and Analysis, the Assistant Secretary of State for Intelligence and Research, the Director of the Office of Intelligence and Counterintelligence of the Department of Energy, the Assistant Secretary for Intelligence and Analysis of the Department of the Treasury, and the Executive Assistant Director for the National Security Branch of the Federal Bureau of Investigation. If the Director does not concur in the recommendation, the department head may not fill the vacancy or make the recommendation to the President, as the case may be. If the department head and the Director do not reach an agreement on the selection or recommendation, the Director and the department head concerned may advise the President directly of the Director's intention to withhold concurrence.

(2) The relevant department head shall consult with the Director before appointing an individual to fill a vacancy or recommending to the President an individual be nominated to fill a vacancy in any of the following positions: the Under Secretary of Defense for Intelligence; the Director of the Defense Intelligence Agency; uniformed heads of the intelligence elements of the Army, the Navy, the Air Force, and the Marine Corps above the rank of Major General or Rear Admiral; the Assistant Commandant of the Coast Guard for Intelligence; and the Assistant Attorney General for National Security.

(e) REMOVAL FROM CERTAIN POSITIONS.

(1) Except for the Director of the Central Intelligence Agency, whose removal the Director may recommend to the President, the Director and the relevant department head shall consult on the removal, or recommendation to the President for removal, as the case may be, of: the Director of the National Security Agency, the Director of the National Geospatial-Intelligence Agency, the Director of the Defense Intelligence Agency, the Under Secretary of Homeland Security for Intelligence and Analysis, the Assistant Secretary of State for Intelligence and Research, and the Assistant Secretary for Intelligence and Analysis of the Department of the Treasury. If the Director and the department head do not agree on removal, or recommendation for removal, either may make a recommendation to the President for the removal of the individual.

(2) The Director and the relevant department or bureau head shall consult on the removal of: the Executive Assistant Director for the National Security Branch of the Federal Bureau of Investigation, the Director of the Office of Intelligence and Counterintelligence of the Department of Energy, the Director of the National Reconnaissance Office, the Assistant Commandant of the Coast Guard for Intelligence, and the Under Secretary of Defense for Intelligence. With respect to an individual appointed by a department head, the department head may remove the individual upon the request of the Director; if the department head chooses not to remove the individual, either the Director or the department head may advise the President of the department head's intention to retain the individual. In the case of the Under Secretary of Defense for Intelligence, the Secretary of Defense may recommend to the President either the removal or the retention of the individual. For uniformed heads of the intelligence elements of the Army, the Navy, the Air Force, and the Marine Corps, the Director may make a recommendation for removal to the Secretary of Defense.

(3) Nothing in this subsection shall be construed to limit or otherwise affect the authority of the President to nominate, appoint, assign, or terminate the appointment or assignment of any individual, with or without a consultation, recommendation, or concurrence.

SEC. 1.4 THE INTELLIGENCE COMMUNITY. Consistent with applicable Federal law and with the other provisions of this order, and under the leadership of the Director, as specified in such law and this order, the Intelligence Community shall:

(a) Collect and provide information needed by the President and, in the performance of executive functions, the Vice President, the NSC, the Homeland

Security Council, the Chairman of the Joint Chiefs of Staff, senior military commanders, and other executive branch officials and, as appropriate, the Congress of the United States;

- (b) In accordance with priorities set by the President, collect information concerning, and conduct activities to protect against, international terrorism, proliferation of weapons of mass destruction, intelligence activities directed against the United States, international criminal drug activities, and other hostile activities directed against the United States by foreign powers, organizations, persons, and their agents;
- (c) Analyze, produce, and disseminate intelligence;
- (d) Conduct administrative, technical, and other support activities within the United States and abroad necessary for the performance of authorized activities, to include providing services of common concern for the Intelligence Community as designated by the Director in accordance with this order;
- (e) Conduct research, development, and procurement of technical systems and devices relating to authorized functions and missions or the provision of services of common concern for the Intelligence Community;
- (f) Protect the security of intelligence related activities, information, installations, property, and employees by appropriate means, including such investigations of applicants, employees, contractors, and other persons with similar associations with the Intelligence Community elements as are necessary;
- (g) Take into account State, local, and tribal governments' and, as appropriate, private sector entities' information needs relating to national and homeland security;
- (h) Deconflict, coordinate, and integrate all intelligence activities and other information gathering in accordance with section 1.3(b)(20) of this order; and
- (i) Perform such other functions and duties related to intelligence activities as the President may direct.

SEC. 1.5 DUTIES AND RESPONSIBILITIES OF THE HEADS OF EXECUTIVE BRANCH DEPARTMENTS AND AGENCIES. The heads of all departments and agencies shall:

- (a) Provide the Director access to all information and intelligence relevant to the national security or that otherwise is required for the performance of the Director's duties, to include administrative and other appropriate management information, except such information excluded by law, by the President, or by the Attorney General acting under this order at the direction of the President;
- (b) Provide all programmatic and budgetary information necessary to support the Director in developing the National Intelligence Program;
- (c) Coordinate development and implementation of intelligence systems and architectures and, as appropriate, operational systems and architectures of their departments, agencies, and other elements with the Director to respond to

- national intelligence requirements and all applicable information sharing and security guidelines, information privacy, and other legal requirements;
- (d) Provide, to the maximum extent permitted by law, subject to the availability of appropriations and not inconsistent with the mission of the department or agency, such further support to the Director as the Director may request, after consultation with the head of the department or agency, for the performance of the Director's functions;
- (e) Respond to advisory tasking from the Director under section 1.3(b)(18) of this order to the greatest extent possible, in accordance with applicable policies established by the head of the responding department or agency;
- (f) Ensure that all elements within the department or agency comply with the provisions of Part 2 of this order, regardless of Intelligence Community affiliation, when performing foreign intelligence and counterintelligence functions;
- (g) Deconflict, coordinate, and integrate all intelligence activities in accordance with section 1.3(b)(20), and intelligence and other activities in accordance with section 1.3(b)(21) of this order;
- (h) Inform the Attorney General, either directly or through the Federal Bureau of Investigation, and the Director of clandestine collection of foreign intelligence and counterintelligence activities inside the United States not coordinated with the Federal Bureau of Investigation;
- (i) Pursuant to arrangements developed by the head of the department or agency and the Director of the Central Intelligence Agency and approved by the Director, inform the Director and the Director of the Central Intelligence Agency, either directly or through his designee serving outside the United States, as appropriate, of clandestine collection of foreign intelligence collected through human sources or through human-enabled means outside the United States that has not been coordinated with the Central Intelligence Agency; and
- (j) Inform the Secretary of Defense, either directly or through his designee, as appropriate, of clandestine collection of foreign intelligence outside the United States in a region of combat or contingency military operations designated by the Secretary of Defense, for purposes of this paragraph, after consultation with the Director of National Intelligence.

SEC. 1.6 HEADS OF ELEMENTS OF THE INTELLIGENCE COMMUNITY. The heads of elements of the Intelligence Community shall:

- (a) Provide the Director access to all information and intelligence relevant to the national security or that otherwise is required for the performance of the Director's duties, to include administrative and other appropriate management information, except such information excluded by law, by the President, or by the Attorney General acting under this order at the direction of the President;

- (b) Report to the Attorney General possible violations of Federal criminal laws by employees and of specified Federal criminal laws by any other person as provided in procedures agreed upon by the Attorney General and the head of the department, agency, or establishment concerned, in a manner consistent with the protection of intelligence sources and methods, as specified in those procedures;
- (c) Report to the Intelligence Oversight Board, consistent with Executive Order 13462 of February 29, 2008, and provide copies of all such reports to the Director, concerning any intelligence activities of their elements that they have reason to believe may be unlawful or contrary to executive order or presidential directive;
- (d) Protect intelligence and intelligence sources, methods, and activities from unauthorized disclosure in accordance with guidance from the Director;
- (e) Facilitate, as appropriate, the sharing of information or intelligence, as directed by law or the President, to State, local, tribal, and private sector entities;
- (f) Disseminate information or intelligence to foreign governments and international organizations under intelligence or counterintelligence arrangements or agreements established in accordance with section 1.3(b)(4) of this order;
- (g) Participate in the development of procedures approved by the Attorney General governing production and dissemination of information or intelligence resulting from criminal drug intelligence activities abroad if they have intelligence responsibilities for foreign or domestic criminal drug production and trafficking; and
- (h) Ensure that the inspectors general, general counsels, and agency officials responsible for privacy or civil liberties protection for their respective organizations have access to any information or intelligence necessary to perform their official duties.

SEC. 1.7 INTELLIGENCE COMMUNITY ELEMENTS. Each element of the Intelligence Community shall have the duties and responsibilities specified below, in addition to those specified by law or elsewhere in this order. Intelligence Community elements within executive departments shall serve the information and intelligence needs of their respective heads of departments and also shall operate as part of an integrated Intelligence Community, as provided in law or this order.

- (a) **THE CENTRAL INTELLIGENCE AGENCY.** The Director of the Central Intelligence Agency shall:
 - (1) Collect (including through clandestine means), analyze, produce, and disseminate foreign intelligence and counterintelligence;
 - (2) Conduct counterintelligence activities without assuming or performing any internal security functions within the United States;

- (3) Conduct administrative and technical support activities within and outside the United States as necessary for cover and proprietary arrangements;
- (4) Conduct covert action activities approved by the President. No agency except the Central Intelligence Agency (or the Armed Forces of the United States in time of war declared by the Congress or during any period covered by a report from the President to the Congress consistent with the War Powers Resolution, Public Law 93-148) may conduct any covert action activity unless the President determines that another agency is more likely to achieve a particular objective;
- (5) Conduct foreign intelligence liaison relationships with intelligence or security services of foreign governments or international organizations consistent with section 1.3(b)(4) of this order;
- (6) Under the direction and guidance of the Director, and in accordance with section 1.3(b)(4) of this order, coordinate the implementation of intelligence and counterintelligence relationships between elements of the Intelligence Community and the intelligence or security services of foreign governments or international organizations; and
- (7) Perform such other functions and duties related to intelligence as the Director may direct.

(b) **THE DEFENSE INTELLIGENCE AGENCY.** The Director of the Defense Intelligence Agency shall:

- (1) Collect (including through clandestine means), analyze, produce, and disseminate foreign intelligence and counterintelligence to support national and departmental missions;
- (2) Collect, analyze, produce, or, through tasking and coordination, provide defense and defense-related intelligence for the Secretary of Defense, the Chairman of the Joint Chiefs of Staff, combatant commanders, other Defense components, and non-Defense agencies;
- (3) Conduct counterintelligence activities;
- (4) Conduct administrative and technical support activities within and outside the United States as necessary for cover and proprietary arrangements;
- (5) Conduct foreign defense intelligence liaison relationships and defense intelligence exchange programs with foreign defense establishments, intelligence or security services of foreign governments, and international organizations in accordance with sections 1.3(b)(4), 1.7(a)(6), and 1.10(i) of this order;
- (6) Manage and coordinate all matters related to the Defense Attaché system; and

(7) Provide foreign intelligence and counterintelligence staff support as directed by the Secretary of Defense.

(c) THE NATIONAL SECURITY AGENCY. The Director of the National Security Agency shall:

(1) Collect (including through clandestine means), process, analyze, produce, and disseminate signals intelligence information and data for foreign intelligence and counterintelligence purposes to support national and departmental missions;

(2) Establish and operate an effective unified organization for signals intelligence activities, except for the delegation of operational control over certain operations that are conducted through other elements of the Intelligence Community. No other department or agency may engage in signals intelligence activities except pursuant to a delegation by the Secretary of Defense, after coordination with the Director;

(3) Control signals intelligence collection and processing activities, including assignment of resources to an appropriate agent for such periods and tasks as required for the direct support of military commanders;

(4) Conduct administrative and technical support activities within and outside the United States as necessary for cover arrangements;

(5) Provide signals intelligence support for national and departmental requirements and for the conduct of military operations;

(6) Act as the National Manager for National Security Systems as established in law and policy, and in this capacity be responsible to the Secretary of Defense and to the Director;

(7) Prescribe, consistent with section 102A(g) of the Act, within its field of authorized operations, security regulations covering operating practices, including the transmission, handling, and distribution of signals intelligence and communications security material within and among the elements under control of the Director of the National Security Agency, and exercise the necessary supervisory control to ensure compliance with the regulations; and

(8) Conduct foreign cryptologic liaison relationships in accordance with sections 1.3(b)(4), 1.7(a)(6), and 1.10(i) of this order.

(d) THE NATIONAL RECONNAISSANCE OFFICE. The Director of the National Reconnaissance Office shall:

(1) Be responsible for research and development, acquisition, launch, deployment, and operation of overhead systems and related data processing facilities to collect intelligence and information to support national and departmental missions and other United States Government needs; and

(2) Conduct foreign liaison relationships relating to the above missions, in accordance with sections 1.3(b)(4), 1.7(a)(6), and 1.10(i) of this order.

(e) THE NATIONAL GEOSPATIAL-INTELLIGENCE AGENCY. The Director of the National Geospatial-Intelligence Agency shall:

(1) Collect, process, analyze, produce, and disseminate geospatial intelligence information and data for foreign intelligence and counterintelligence purposes to support national and departmental missions;

(2) Provide geospatial intelligence support for national and departmental requirements and for the conduct of military operations;

(3) Conduct administrative and technical support activities within and outside the United States as necessary for cover arrangements; and

(4) Conduct foreign geospatial intelligence liaison relationships, in accordance with sections 1.3(b)(4), 1.7(a)(6), and 1.10(i) of this order.

(f) THE INTELLIGENCE AND COUNTERINTELLIGENCE ELEMENTS OF THE ARMY, NAVY, AIR FORCE, AND MARINE CORPS. The Commanders and heads of the intelligence and counterintelligence elements of the Army, Navy, Air Force, and Marine Corps shall:

(1) Collect (including through clandestine means), produce, analyze, and disseminate defense and defense-related intelligence and counterintelligence to support departmental requirements, and, as appropriate, national requirements;

(2) Conduct counterintelligence activities;

(3) Monitor the development, procurement, and management of tactical intelligence systems and equipment and conduct related research, development, and test and evaluation activities; and

(4) Conduct military intelligence liaison relationships and military intelligence exchange programs with selected cooperative foreign defense establishments and international organizations in accordance with sections 1.3(b)(4), 1.7(a)(6), and 1.10(i) of this order.

(g) INTELLIGENCE ELEMENTS OF THE FEDERAL BUREAU OF INVESTIGATION. Under the supervision of the Attorney General and pursuant to such regulations as the Attorney General may establish, the intelligence elements of the Federal Bureau of Investigation shall:

(1) Collect (including through clandestine means), analyze, produce, and disseminate foreign intelligence and counterintelligence to support national and departmental missions, in accordance with procedural guidelines approved by the Attorney General, after consultation with the Director;

(2) Conduct counterintelligence activities; and

(3) Conduct foreign intelligence and counterintelligence liaison relationships with intelligence, security, and law enforcement services of foreign governments or international organizations in accordance with sections 1.3(b)(4) and 1.7(a)(6) of this order.

(h) THE INTELLIGENCE AND COUNTERINTELLIGENCE ELEMENTS OF THE COAST GUARD. The Commandant of the Coast Guard shall:

(1) Collect (including through clandestine means), analyze, produce, and disseminate foreign intelligence and counterintelligence including defense and defense-related information and intelligence to support national and departmental missions;

(2) Conduct counterintelligence activities;

(3) Monitor the development, procurement, and management of tactical intelligence systems and equipment and conduct related research, development, and test and evaluation activities; and

(4) Conduct foreign intelligence liaison relationships and intelligence exchange programs with foreign intelligence services, security services or international organizations in accordance with sections 1.3(b)(4), 1.7(a)(6), and, when operating as part of the Department of Defense, 1.10(i) of this order.

(i) THE BUREAU OF INTELLIGENCE AND RESEARCH, DEPARTMENT OF STATE; THE OFFICE OF INTELLIGENCE AND ANALYSIS, DEPARTMENT OF THE TREASURY; THE OFFICE OF NATIONAL SECURITY INTELLIGENCE, DRUG ENFORCEMENT ADMINISTRATION; THE OFFICE OF INTELLIGENCE AND ANALYSIS, DEPARTMENT OF HOMELAND SECURITY; AND THE OFFICE OF INTELLIGENCE AND COUNTERINTELLIGENCE, DEPARTMENT OF ENERGY. The heads of the Bureau of Intelligence and Research, Department of State; the Office of Intelligence and Analysis, Department of the Treasury; the Office of National Security Intelligence, Drug Enforcement Administration; the Office of Intelligence and Analysis, Department of Homeland Security; and the Office of Intelligence and Counterintelligence, Department of Energy shall:

(1) Collect (overtly or through publicly available sources), analyze, produce, and disseminate information, intelligence, and counterintelligence to support national and departmental missions; and

(2) Conduct and participate in analytic or information exchanges with foreign partners and international organizations in accordance with sections 1.3(b)(4) and 1.7(a)(6) of this order.

(j) THE OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE. The Director shall collect (overtly or through publicly available sources), analyze, produce, and disseminate information, intelligence, and counterintelligence to support the missions of the Office of the Director of National Intelligence,

including the National Counterterrorism Center, and to support other national missions.

SEC. 1.8 THE DEPARTMENT OF STATE. In addition to the authorities exercised by the Bureau of Intelligence and Research under sections 1.4 and 1.7(i) of this order, the Secretary of State shall:

- (a) Collect (overtly or through publicly available sources) information relevant to United States foreign policy and national security concerns;
- (b) Disseminate, to the maximum extent possible, reports received from United States diplomatic and consular posts;
- (c) Transmit reporting requirements and advisory taskings of the Intelligence Community to the Chiefs of United States Missions abroad; and
- (d) Support Chiefs of United States Missions in discharging their responsibilities pursuant to law and presidential direction.

SEC. 1.9 THE DEPARTMENT OF THE TREASURY. In addition to the authorities exercised by the Office of Intelligence and Analysis of the Department of the Treasury under sections 1.4 and 1.7(i) of this order the Secretary of the Treasury shall collect (overtly or through publicly available sources) foreign financial information and, in consultation with the Department of State, foreign economic information.

SEC. 1.10 THE DEPARTMENT OF DEFENSE. The Secretary of Defense shall:

- (a) Collect (including through clandestine means), analyze, produce, and disseminate information and intelligence and be responsive to collection tasking and advisory tasking by the Director;
- (b) Collect (including through clandestine means), analyze, produce, and disseminate defense and defense-related intelligence and counterintelligence, as required for execution of the Secretary's responsibilities;
- (c) Conduct programs and missions necessary to fulfill national, departmental, and tactical intelligence requirements;
- (d) Conduct counterintelligence activities in support of Department of Defense components and coordinate counterintelligence activities in accordance with section 1.3(b)(20) and (21) of this order;
- (e) Act, in coordination with the Director, as the executive agent of the United States Government for signals intelligence activities;
- (f) Provide for the timely transmission of critical intelligence, as defined by the Director, within the United States Government;
- (g) Carry out or contract for research, development, and procurement of technical systems and devices relating to authorized intelligence functions;

- (h) Protect the security of Department of Defense installations, activities, information, property, and employees by appropriate means, including such investigations of applicants, employees, contractors, and other persons with similar associations with the Department of Defense as are necessary;
- (i) Establish and maintain defense intelligence relationships and defense intelligence exchange programs with selected cooperative foreign defense establishments, intelligence or security services of foreign governments, and international organizations, and ensure that such relationships and programs are in accordance with sections 1.3(b)(4), 1.3(b)(21) and 1.7(a)(6) of this order;
- (j) Conduct such administrative and technical support activities within and outside the United States as are necessary to provide for cover and proprietary arrangements, to perform the functions described in sections (a) through (i) above, and to support the Intelligence Community elements of the Department of Defense; and
- (k) Use the Intelligence Community elements within the Department of Defense identified in section 1.7(b) through (f) and, when the Coast Guard is operating as part of the Department of Defense, (h) above to carry out the Secretary of Defense's responsibilities assigned in this section or other departments, agencies, or offices within the Department of Defense, as appropriate, to conduct the intelligence missions and responsibilities assigned to the Secretary of Defense.

SEC. 1.11 THE DEPARTMENT OF HOMELAND SECURITY. In addition to the authorities exercised by the Office of Intelligence and Analysis of the Department of Homeland Security under sections 1.4 and 1.7(i) of this order, the Secretary of Homeland Security shall conduct, through the United States Secret Service, activities to determine the existence and capability of surveillance equipment being used against the President or the Vice President of the United States, the Executive Office of the President, and, as authorized by the Secretary of Homeland Security or the President, other Secret Service protectees and United States officials. No information shall be acquired intentionally through such activities except to protect against use of such surveillance equipment, and those activities shall be conducted pursuant to procedures agreed upon by the Secretary of Homeland Security and the Attorney General.

SEC. 1.12 THE DEPARTMENT OF ENERGY. In addition to the authorities exercised by the Office of Intelligence and Counterintelligence of the Department of Energy under sections 1.4 and 1.7(i) of this order, the Secretary of Energy shall:

- (a) Provide expert scientific, technical, analytic, and research capabilities to other agencies within the Intelligence Community, as appropriate;
- (b) Participate in formulating intelligence collection and analysis requirements where the special expert capability of the Department can contribute; and

(c) Participate with the Department of State in overtly collecting information with respect to foreign energy matters.

SEC. 1.13 THE FEDERAL BUREAU OF INVESTIGATION. In addition to the authorities exercised by the intelligence elements of the Federal Bureau of Investigation of the Department of Justice under sections 1.4 and 1.7(g) of this order and under the supervision of the Attorney General and pursuant to such regulations as the Attorney General may establish, the Director of the Federal Bureau of Investigation shall provide technical assistance, within or outside the United States, to foreign intelligence and law enforcement services, consistent with section 1.3(b)(20) and (21) of this order, as may be necessary to support national or departmental missions.

PART 2 – CONDUCT OF INTELLIGENCE ACTIVITIES

SEC. 2.1 NEED. Timely, accurate, and insightful information about the activities, capabilities, plans, and intentions of foreign powers, organizations, and persons, and their agents, is essential to informed decisionmaking in the areas of national security, national defense, and foreign relations. Collection of such information is a priority objective and will be pursued in a vigorous, innovative, and responsible manner that is consistent with the Constitution and applicable law and respectful of the principles upon which the United States was founded.

SEC. 2.2 PURPOSE. This Order is intended to enhance human and technical collection techniques, especially those undertaken abroad, and the acquisition of significant foreign intelligence, as well as the detection and countering of international terrorist activities, the spread of weapons of mass destruction, and espionage conducted by foreign powers. Set forth below are certain general principles that, in addition to and consistent with applicable laws, are intended to achieve the proper balance between the acquisition of essential information and protection of individual interests. Nothing in this Order shall be construed to apply to or interfere with any authorized civil or criminal law enforcement responsibility of any department or agency.

SEC. 2.3 COLLECTION OF INFORMATION. Elements of the Intelligence Community are authorized to collect, retain, or disseminate information concerning United States persons only in accordance with procedures established by the head of the Intelligence Community element concerned or by the head of a department containing such element and approved by the Attorney General, consistent with the authorities provided by Part 1 of this Order, after consultation

with the Director. Those procedures shall permit collection, retention, and dissemination of the following types of information:

- (a) Information that is publicly available or collected with the consent of the person concerned;
- (b) Information constituting foreign intelligence or counterintelligence, including such information concerning corporations or other commercial organizations. Collection within the United States of foreign intelligence not otherwise obtainable shall be undertaken by the Federal Bureau of Investigation (FBI) or, when significant foreign intelligence is sought, by other authorized elements of the Intelligence Community, provided that no foreign intelligence collection by such elements may be undertaken for the purpose of acquiring information concerning the domestic activities of United States persons;
- (c) Information obtained in the course of a lawful foreign intelligence, counterintelligence, international drug or international terrorism investigation;
- (d) Information needed to protect the safety of any persons or organizations, including those who are targets, victims, or hostages of international terrorist organizations;
- (e) Information needed to protect foreign intelligence or counterintelligence sources, methods, and activities from unauthorized disclosure. Collection within the United States shall be undertaken by the FBI except that other elements of the Intelligence Community may also collect such information concerning present or former employees, present or former intelligence element contractors or their present or former employees, or applicants for such employment or contracting;
- (f) Information concerning persons who are reasonably believed to be potential sources or contacts for the purpose of determining their suitability or credibility;
- (g) Information arising out of a lawful personnel, physical, or communications security investigation;
- (h) Information acquired by overhead reconnaissance not directed at specific United States persons;
- (i) Incidentally obtained information that may indicate involvement in activities that may violate Federal, state, local, or foreign laws; and
- (j) Information necessary for administrative purposes.

In addition, elements of the Intelligence Community may disseminate information to each appropriate element within the Intelligence Community for purposes of allowing the recipient element to determine whether the information is relevant to its responsibilities and can be retained by it, except that information derived from signals intelligence may only be disseminated or made available to Intelligence Community elements in accordance with procedures established by the Director in coordination with the Secretary of Defense and approved by the Attorney General.

SEC. 2.4 COLLECTION TECHNIQUES. Elements of the Intelligence Community shall use the least intrusive collection techniques feasible within the United States or directed against United States persons abroad. Elements of the Intelligence Community are not authorized to use such techniques as electronic surveillance, unconsented physical searches, mail surveillance, physical surveillance, or monitoring devices unless they are in accordance with procedures established by the head of the Intelligence Community element concerned or the head of a department containing such element and approved by the Attorney General, after consultation with the Director. Such procedures shall protect constitutional and other legal rights and limit use of such information to lawful governmental purposes. These procedures shall not authorize:

(a) The Central Intelligence Agency (CIA) to engage in electronic surveillance within the United States except for the purpose of training, testing, or conducting countermeasures to hostile electronic surveillance;

(b) Unconsented physical searches in the United States by elements of the Intelligence Community other than the FBI, except for:

(1) Searches by counterintelligence elements of the military services directed against military personnel within the United States or abroad for intelligence purposes, when authorized by a military commander empowered to approve physical searches for law enforcement purposes, based upon a finding of probable cause to believe that such persons are acting as agents of foreign powers; and

(2) Searches by CIA of personal property of non-United States persons lawfully in its possession;

(c) Physical surveillance of a United States person in the United States by elements of the Intelligence Community other than the FBI, except for:

(1) Physical surveillance of present or former employees, present or former intelligence element contractors or their present or former employees, or applicants for any such employment or contracting; and

(2) Physical surveillance of a military person employed by a non-intelligence element of a military service; and

(d) Physical surveillance of a United States person abroad to collect foreign intelligence, except to obtain significant information that cannot reasonably be acquired by other means.

SEC. 2.5 ATTORNEY GENERAL APPROVAL. The Attorney General hereby is delegated the power to approve the use for intelligence purposes, within the United States or against a United States person abroad, of any technique for which a warrant would be required if undertaken for law enforcement purposes, provided that such techniques shall not be undertaken unless the Attorney General has determined in each case that there is probable cause to believe that

the technique is directed against a foreign power or an agent of a foreign power. The authority delegated pursuant to this paragraph, including the authority to approve the use of electronic surveillance as defined in the Foreign Intelligence Surveillance Act of 1978, as amended, shall be exercised in accordance with that Act.

SEC. 2.6 ASSISTANCE TO LAW ENFORCEMENT AND OTHER CIVIL AUTHORITIES.

Elements of the Intelligence Community are authorized to:

- (a) Cooperate with appropriate law enforcement agencies for the purpose of protecting the employees, information, property, and facilities of any element of the Intelligence Community;
- (b) Unless otherwise precluded by law or this Order, participate in law enforcement activities to investigate or prevent clandestine intelligence activities by foreign powers, or international terrorist or narcotics activities;
- (c) Provide specialized equipment, technical knowledge, or assistance of expert personnel for use by any department or agency, or when lives are endangered, to support local law enforcement agencies. Provision of assistance by expert personnel shall be approved in each case by the general counsel of the providing element or department; and
- (d) Render any other assistance and cooperation to law enforcement or other civil authorities not precluded by applicable law.

SEC. 2.7 CONTRACTING. Elements of the Intelligence Community are authorized to enter into contracts or arrangements for the provision of goods or services with private companies or institutions in the United States and need not reveal the sponsorship of such contracts or arrangements for authorized intelligence purposes. Contracts or arrangements with academic institutions may be undertaken only with the consent of appropriate officials of the institution.

SEC. 2.8 CONSISTENCY WITH OTHER LAWS. Nothing in this Order shall be construed to authorize any activity in violation of the Constitution or statutes of the United States.

SEC. 2.9 UNDISCLOSED PARTICIPATION IN ORGANIZATIONS WITHIN THE UNITED STATES. No one acting on behalf of elements of the Intelligence Community may join or otherwise participate in any organization in the United States on behalf of any element of the Intelligence Community without disclosing such person's intelligence affiliation to appropriate officials of the organization, except in accordance with procedures established by the head of the Intelligence Community element concerned or the head of a department containing such element and approved by the Attorney General, after consultation with the

Director. Such participation shall be authorized only if it is essential to achieving lawful purposes as determined by the Intelligence Community element head or designee. No such participation may be undertaken for the purpose of influencing the activity of the organization or its members except in cases where:

- (a) The participation is undertaken on behalf of the FBI in the course of a lawful investigation; or
- (b) The organization concerned is composed primarily of individuals who are not United States persons and is reasonably believed to be acting on behalf of a foreign power.

SEC. 2.10 HUMAN EXPERIMENTATION. No element of the Intelligence Community shall sponsor, contract for, or conduct research on human subjects except in accordance with guidelines issued by the Department of Health and Human Services. The subject's informed consent shall be documented as required by those guidelines.

SEC. 2.11 PROHIBITION ON ASSASSINATION. No person employed by or acting on behalf of the United States Government shall engage in or conspire to engage in assassination.

SEC. 2.12 INDIRECT PARTICIPATION. No element of the Intelligence Community shall participate in or request any person to undertake activities forbidden by this Order.

SEC. 2.13 LIMITATION ON COVERT ACTION. No covert action may be conducted which is intended to influence United States political processes, public opinion, policies, or media.

PART 3 – GENERAL PROVISIONS

SEC. 3.1 CONGRESSIONAL OVERSIGHT. The duties and responsibilities of the Director and the heads of other departments, agencies, elements, and entities engaged in intelligence activities to cooperate with the Congress in the conduct of its responsibilities for oversight of intelligence activities shall be implemented in accordance with applicable law, including title V of the Act. The requirements of applicable law, including title V of the Act, shall apply to all covert action activities as defined in this Order.

SEC. 3.2 IMPLEMENTATION. The President, supported by the NSC, and the Director shall issue such appropriate directives, procedures, and guidance as are necessary to implement this order. Heads of elements within the Intelligence

Community shall issue appropriate procedures and supplementary directives consistent with this order. No procedures to implement Part 2 of this order shall be issued without the Attorney General's approval, after consultation with the Director. The Attorney General shall provide a statement of reasons for not approving any procedures established by the head of an element in the Intelligence Community (or the head of the department containing such element) other than the FBI. In instances where the element head or department head and the Attorney General are unable to reach agreements on other than constitutional or other legal grounds, the Attorney General, the head of department concerned, or the Director shall refer the matter to the NSC.

SEC. 3.3 PROCEDURES. The activities herein authorized that require procedures shall be conducted in accordance with existing procedures or requirements established under Executive Order 12333. New procedures, as required by Executive Order 12333, as further amended, shall be established as expeditiously as possible. All new procedures promulgated pursuant to Executive Order 12333, as amended, shall be made available to the Select Committee on Intelligence of the Senate and the Permanent Select Committee on Intelligence of the House of Representatives.

SEC. 3.4 REFERENCES AND TRANSITION. References to "Senior Officials of the Intelligence Community" or "SOICs" in executive orders or other Presidential guidance, shall be deemed references to the heads of elements in the Intelligence Community, unless the President otherwise directs; references in Intelligence Community or Intelligence Community element policies or guidance, shall be deemed to be references to the heads of elements of the Intelligence Community, unless the President or the Director otherwise directs.

SEC. 3.5 DEFINITIONS. For the purposes of this Order, the following terms shall have these meanings:

(a) *Counterintelligence* means information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, or persons, or their agents, or international terrorist organizations or activities.

(b) *Covert action* means an activity or activities of the United States Government to influence political, economic, or military conditions abroad, where it is intended that the role of the United States Government will not be apparent or acknowledged publicly, but does not include:

(1) Activities the primary purpose of which is to acquire intelligence, traditional counterintelligence activities, traditional activities to improve

or maintain the operational security of United States Government programs, or administrative activities;

(2) Traditional diplomatic or military activities or routine support to such activities;

(3) Traditional law enforcement activities conducted by United States Government law enforcement agencies or routine support to such activities; or

(4) Activities to provide routine support to the overt activities (other than activities described in paragraph (1), (2), or (3)) of other United States Government agencies abroad.

(c) *Electronic surveillance* means acquisition of a nonpublic communication by electronic means without the consent of a person who is a party to an electronic communication or, in the case of a nonelectronic communication, without the consent of a person who is visibly present at the place of communication, but not including the use of radio direction-finding equipment solely to determine the location of a transmitter.

(d) *Employee* means a person employed by, assigned or detailed to, or acting for an element within the Intelligence Community.

(e) *Foreign intelligence* means information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, foreign persons, or international terrorists.

(f) *Intelligence* includes foreign intelligence and counterintelligence.

(g) *Intelligence activities* means all activities that elements of the Intelligence Community are authorized to conduct pursuant to this order.

(h) *Intelligence Community* and elements of the Intelligence Community refers to:

(1) The Office of the Director of National Intelligence;

(2) The Central Intelligence Agency;

(3) The National Security Agency;

(4) The Defense Intelligence Agency;

(5) The National Geospatial-Intelligence Agency;

(6) The National Reconnaissance Office;

(7) The other offices within the Department of Defense for the collection of specialized national foreign intelligence through reconnaissance programs;

(8) The intelligence and counterintelligence elements of the Army, the Navy, the Air Force, and the Marine Corps;

(9) The intelligence elements of the Federal Bureau of Investigation;

(10) The Office of National Security Intelligence of the Drug Enforcement Administration;

- (11) The Office of Intelligence and Counterintelligence of the Department of Energy;
- (12) The Bureau of Intelligence and Research of the Department of State;
- (13) The Office of Intelligence and Analysis of the Department of the Treasury;
- (14) The Office of Intelligence and Analysis of the Department of Homeland Security;
- (15) The intelligence and counterintelligence elements of the Coast Guard; and
- (16) Such other elements of any department or agency as may be designated by the President, or designated jointly by the Director and the head of the department or agency concerned, as an element of the Intelligence Community.

(i) *National Intelligence and Intelligence Related to National Security* means all intelligence, regardless of the source from which derived and including information gathered within or outside the United States, that pertains, as determined consistent with any guidance issued by the President, or that is determined for the purpose of access to information by the Director in accordance with section 1.3(a)(1) of this order, to pertain to more than one United States Government agency; and that involves threats to the United States, its people, property, or interests; the development, proliferation, or use of weapons of mass destruction; or any other matter bearing on United States national or homeland security.

(j) *The National Intelligence Program* means all programs, projects, and activities of the Intelligence Community, as well as any other programs of the Intelligence Community designated jointly by the Director and the head of a United States department or agency or by the President. Such term does not include programs, projects, or activities of the military departments to acquire intelligence solely for the planning and conduct of tactical military operations by United States Armed Forces.

(k) *United States person* means a United States citizen, an alien known by the intelligence element concerned to be a permanent resident alien, an unincorporated association substantially composed of United States citizens or permanent resident aliens, or a corporation incorporated in the United States, except for a corporation directed and controlled by a foreign government or governments.

SEC. 3.6 REVOCATION. Executive Orders 13354 and 13355 of August 27, 2004, are revoked; and paragraphs 1.3(b)(9) and (10) of Part 1 supersede provisions within Executive Order 12958, as amended, to the extent such provisions in Executive Order 12958, as amended, are inconsistent with this Order.

SEC. 3.7 GENERAL PROVISIONS.

(a) Consistent with section 1.3(c) of this order, nothing in this order shall be construed to impair or otherwise affect:

(1) Authority granted by law to a department or agency, or the head thereof; or

(2) Functions of the Director of the Office of Management and Budget relating to budget, administrative, or legislative proposals.

(b) This order shall be implemented consistent with applicable law and subject to the availability of appropriations.

(c) This order is intended only to improve the internal management of the executive branch and is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity, by any party against the United States, its departments, agencies or entities, its officers, employees, or agents, or any other person.

-/S/- Ronald Reagan
THE WHITE HOUSE,
December 4, 1981.

EXECUTIVE ORDER 12949:
FOREIGN INTELLIGENCE PHYSICAL SEARCHES

[Signed: February 9, 1995, Federal Register Vol. 60, No. 29 (February 13, 1995), as amended by EO 13475 (2008)]

By the authority vested in me as President by the Constitution and the laws of the United States, including sections 302 and 303 of the Foreign Intelligence Surveillance Act of 1978 (“Act”) (50 U.S.C. 1801, *et seq.*), as amended by Public Law 103–359, and in order to provide for the authorization of physical searches for foreign intelligence purposes as set forth in the Act, it is hereby ordered as follows:

SECTION 1. Pursuant to section 302(a)(1) of the Act, the Attorney General is authorized to approve physical searches, without a court order, to acquire foreign intelligence information for periods of up to one year, if the Attorney General makes the certifications required by that section.

SEC. 2. Pursuant to section 302(b) of the Act, the Attorney General is authorized to approve applications to the Foreign Intelligence Surveillance Court under section 303 of the Act to obtain orders for physical searches for the purpose of collecting foreign intelligence information.

SEC. 3. Pursuant to section 303(a)(6) of the Act, the following officials, each of whom is employed in the area of national security or defense, is designated to make the certifications required by section 303(a)(6) of the Act in support of applications to conduct physical searches:

- (a) Secretary of State;
- (b) Secretary of Defense;
- (c) Director of National Intelligence;
- (d) Director of the Federal Bureau of Investigation;
- (e) Deputy Secretary of State;
- (f) Deputy Secretary of Defense;
- (g) Director of the Central Intelligence Agency
- (h) Principal Deputy Director of National Intelligence; and
- (i) Deputy Director of the Federal Bureau of Investigation.

None of the above officials, nor anyone officially acting in that capacity, may exercise the authority to make the above certifications, unless that official has been appointed by the President, by and with the advice and consent of the Senate. The requirement of the preceding sentence that the named official must

EXECUTIVE ORDER 12949, FOREIGN INTELLIGENCE PHYSICAL SEARCHES

be appointed by the President with the advice and consent of the Senate does not apply to the Deputy Director of the Federal Bureau of Investigation.

-/S/- William J. Clinton
THE WHITE HOUSE,
February 9, 1995.

EXECUTIVE ORDER 12968:
ACCESS TO CLASSIFIED INFORMATION

[Signed: August 2, 1995, Federal Register Vol. 60, No. 151 (August 7, 1995),
as amended by EO 13467 (2008)]

The national interest requires that certain information be maintained in confidence through a system of classification in order to protect our citizens, our democratic institutions, and our participation within the community of nations. The unauthorized disclosure of information classified in the national interest can cause irreparable damage to the national security and loss of human life.

Security policies designed to protect classified information must ensure consistent, cost effective, and efficient protection of our Nation's classified information, while providing fair and equitable treatment to those Americans upon whom we rely to guard our national security.

This order establishes a uniform Federal personnel security program for employees who will be considered for initial or continued access to classified information.

NOW, THEREFORE, by the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

**PART 1—DEFINITIONS, ACCESS TO CLASSIFIED INFORMATION,
FINANCIAL DISCLOSURE, AND OTHER ITEMS**

SECTION 1.1. DEFINITIONS.

For the purposes of this order:

- (a) "Agency" means any "Executive agency," as defined in 5 U.S.C. § 105, the "military departments," as defined in 5 U.S.C. § 102, and any other entity within the executive branch that comes into the possession of classified information, including the Defense Intelligence Agency, National Security Agency, and the National Reconnaissance Office.
- (b) "Applicant" means a person other than an employee who has received an authorized conditional offer of employment for a position that requires access to classified information.
- (c) "Authorized investigative agency" means an agency authorized by law or regulation to conduct a counterintelligence investigation or investigation of persons who are proposed for access to classified information to ascertain

whether such persons satisfy the criteria for obtaining and retaining access to such information.

(d) “Classified information” means information that has been determined pursuant to Executive Order No. 12958, or any successor order, Executive Order No. 12951, or any successor order, or the Atomic Energy Act of 1954 (42 U.S.C. § 2011), to require protection against unauthorized disclosure.

(e) “Employee” means a person, other than the President and Vice President, employed by, detailed or assigned to, an agency, including members of the Armed Forces; an expert or consultant to an agency; an industrial or commercial contractor, licensee, certificate holder, or grantee of an agency, including all subcontractors; a personal services contractor; or any other category of person who acts for or on behalf of an agency as determined by the appropriate agency head.

(f) “Foreign power” and “agent of a foreign power” have the meaning provided in 50 U.S.C. § 1801.

(g) “Need for access” means a determination that an employee requires access to a particular level of classified information in order to perform or assist in a lawful and authorized governmental function.

(h) “Need-to-know” means a determination made by an authorized holder of classified information that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function.

(i) “Overseas Security Policy Board” means the Board established by the President to consider, develop, coordinate and promote policies, standards and agreements on overseas security operations, programs and projects that affect all United States Government agencies under the authority of a Chief of Mission.

(j) “Security Executive Agent” means the Board established by the President to consider, coordinate, and recommend policy directives for U.S. security policies, procedures, and practices.

(k) “Special access program” has the meaning provided in section 4.1 of Executive Order No. 12958, or any successor order.

SEC. 1.2. ACCESS TO CLASSIFIED INFORMATION.

(a) No employee shall be granted access to classified information unless that employee has been determined to be eligible in accordance with this order and to possess a need-to-know.

(b) Agency heads shall be responsible for establishing and maintaining an effective program to ensure that access to classified information by each employee is clearly consistent with the interests of the national security.

(c) Employees shall not be granted access to classified information unless they:

(1) have been determined to be eligible for access under section 3.1 of this order by agency heads or designated officials based upon a favorable adjudication of an appropriate investigation of the employee's background;

(2) have a demonstrated need-to-know; and

(3) have signed an approved nondisclosure agreement.

(d) All employees shall be subject to investigation by an appropriate government authority prior to being granted access to classified information and at any time during the period of access to ascertain whether they continue to meet the requirements for access.

(e)(1) All employees granted access to classified information shall be required as a condition of such access to provide to the employing agency written consent permitting access by an authorized investigative agency, for such time as access to classified information is maintained and for a period of 3 years thereafter, to:

(A) relevant financial records that are maintained by a financial institution as defined in 31 U.S.C. § 5312(a) or by a holding company as defined in section 1101(6) of the Right to Financial Privacy Act of 1978 (12 U.S.C. § 3401);

(B) consumer reports pertaining to the employee under the Fair Credit Reporting Act (15 U.S.C. § 1681a); and

(C) records maintained by commercial entities within the United States pertaining to any travel by the employee outside the United States.

(2) Information may be requested pursuant to employee consent under this section where:

(A) there are reasonable grounds to believe, based on credible information, that the employee or former employee is, or may be, disclosing classified information in an unauthorized manner to a foreign power or agent of a foreign power;

(B) information the employing agency deems credible indicates the employee or former employee has incurred excessive indebtedness or has acquired a level of affluence that cannot be explained by other information; or

(C) circumstances indicate the employee or former employee had the capability and opportunity to disclose classified information that is known to have been lost or compromised to a foreign power or an agent of a foreign power.

(3) Nothing in this section shall be construed to affect the authority of an investigating agency to obtain information pursuant to the Right to Financial Privacy Act, the Fair Credit Reporting Act or any other applicable law.

SEC. 1.3. FINANCIAL DISCLOSURE.

(a) Not later than 180 days after the effective date of this order, the head of each agency that originates, handles, transmits, or possesses classified information shall designate each employee, by position or category where possible, who has a regular need for access to classified information that, in the discretion of the agency head, would reveal:

- (1) the identity of covert agents as defined in the Intelligence Identities Protection Act of 1982 [50 U.S.C. § 3121];
- (2) technical or specialized national intelligence collection and processing systems that, if disclosed in an unauthorized manner, would substantially negate or impair the effectiveness of the system;
- (3) the details of:
 - (A) the nature, contents, algorithm, preparation, or use of any code, cipher, or cryptographic system or;
 - (B) the design, construction, functioning, maintenance, or repair of any cryptographic equipment; but not including information concerning the use of cryptographic equipment and services;
- (4) particularly sensitive special access programs, the disclosure of which would substantially negate or impair the effectiveness of the information or activity involved; or
- (5) especially sensitive nuclear weapons design information (but only for those positions that have been certified as being of a high degree of importance or sensitivity, as described in section 145(f) of the Atomic Energy Act of 1954, as amended).

(b) An employee may not be granted access, or hold a position designated as requiring access, to information described in subsection (a) unless, as a condition of access to such information, the employee:

- (1) files with the head of the agency a financial disclosure report, including information with respect to the spouse and dependent children of the employee, as part of all background investigations or reinvestigations;
- (2) is subject to annual financial disclosure requirements, if selected by the agency head; and
- (3) files relevant information concerning foreign travel, as determined by the Security Executive Agent.

(c) Not later than 180 days after the effective date of this order, the Security Executive Agent shall develop procedures for the implementation of this section, including a standard financial disclosure form for use by employees under subsection (b) of this section, and agency heads shall identify certain employees, by position or category, who are subject to annual financial disclosure.

SEC. 1.4. USE OF AUTOMATED FINANCIAL RECORD DATA BASES.

As part of all investigations and reinvestigations described in section 1.2(d) of this order, agencies may request the Department of the Treasury, under terms and conditions prescribed by the Secretary of the Treasury, to search automated data bases consisting of reports of currency transactions by financial institutions, international transportation of currency or monetary instruments, foreign bank and financial accounts, transactions under \$10,000 that are reported as possible money laundering violations, and records of foreign travel.

SEC. 1.5. EMPLOYEE EDUCATION AND ASSISTANCE.

The head of each agency that grants access to classified information shall establish a program for employees with access to classified information to:

- (a) educate employees about individual responsibilities under this order; and
- (b) inform employees about guidance and assistance available concerning issues that may affect their eligibility for access to classified information, including sources of assistance for employees who have questions or concerns about financial matters, mental health, or substance abuse.

PART 2—ACCESS ELIGIBILITY POLICY AND PROCEDURE

SEC. 2.1. ELIGIBILITY DETERMINATIONS.

(a) Determinations of eligibility for access to classified information shall be based on criteria established under this order. Such determinations are separate from suitability determinations with respect to the hiring or retention of persons for employment by the government or any other personnel actions.

(b) The number of employees that each agency determines are eligible for access to classified information shall be kept to the minimum required for the conduct of agency functions.

(1) Eligibility for access to classified information shall not be requested or granted solely to permit entry to, or ease of movement within, controlled areas when the employee has no need for access and access to classified information may reasonably be prevented. Where circumstances indicate employees may be inadvertently exposed to classified information in the course of their duties, agencies are authorized to grant or deny, in their discretion, facility access approvals to such employees based on an appropriate level of investigation as determined by each agency.

(2) Except in agencies where eligibility for access is a mandatory condition of employment, eligibility for access to classified information shall only be requested or granted based on a demonstrated, foreseeable

need for access. Requesting or approving eligibility in excess of actual requirements is prohibited.

(3) Eligibility for access to classified information may be granted where there is a temporary need for access, such as one-time participation in a classified project, provided the investigative standards established under this order have been satisfied. In such cases, a fixed date or event for expiration shall be identified and access to classified information shall be limited to information related to the particular project or assignment.

(4) Access to classified information shall be terminated when an employee no longer has a need for access.

SEC. 2.2. LEVEL OF ACCESS APPROVAL.

(a) The level at which an access approval is granted for an employee shall be limited, and relate directly, to the level of classified information for which there is a need for access. Eligibility for access to a higher level of classified information includes eligibility for access to information classified at a lower level.

(b) Access to classified information relating to a special access program shall be granted in accordance with procedures established by the head of the agency that created the program or, for programs pertaining to intelligence activities (including special activities but not including military operational, strategic, and tactical programs) or intelligence sources and methods, by the Director of Central Intelligence. To the extent possible and consistent with the national security interests of the United States, such procedures shall be consistent with the standards and procedures established by and under this order.

SEC. 2.3 TEMPORARY ACCESS TO HIGHER LEVELS.

(a) An employee who has been determined to be eligible for access to classified information based on favorable adjudication of a completed investigation may be granted temporary access to a higher level where security personnel authorized by the agency head to make access eligibility determinations find that such access:

- (1) is necessary to meet operational or contractual exigencies not expected to be of a recurring nature;
- (2) will not exceed 180 days; and
- (3) is limited to specific, identifiable information that is made the subject of a written access record.

(b) Where the access granted under subsection (a) of this section involves another agency's classified information, that agency must concur before access to its information is granted.

SEC. 2.4. RECIPROCAL ACCEPTANCE OF ACCESS ELIGIBILITY DETERMINATIONS.

(a) Except when an agency has substantial information indicating that an employee may not satisfy the standards in section 3.1 of this order, background investigations and eligibility determinations conducted under this order shall be mutually and reciprocally accepted by all agencies.

(b) Except where there is substantial information indicating that the employee may not satisfy the standards in section 3.1 of this order, an employee with existing access to a special access program shall not be denied eligibility for access to another special access program at the same sensitivity level as determined personally by the agency head or deputy agency head, or have an existing access eligibility readjudicated, so long as the employee has a need for access to the information involved.

(c) This section shall not preclude agency heads from establishing additional, but not duplicative, investigative or adjudicative procedures for a special access program or for candidates for detail or assignment to their agencies, where such procedures are required in exceptional circumstances to protect the national security.

(d) Where temporary eligibility for access is granted under sections 2.3 or 3.3 of this order or where the determination of eligibility for access is conditional, the fact of such temporary or conditional access shall be conveyed to any other agency that considers affording the employee access to its information.

SEC. 2.5. SPECIFIC ACCESS REQUIREMENT.

(a) Employees who have been determined to be eligible for access to classified information shall be given access to classified information only where there is a need-to-know that information.

(b) It is the responsibility of employees who are authorized holders of classified information to verify that a prospective recipient's eligibility for access has been granted by an authorized agency official and to ensure that a need-to-know exists prior to allowing such access, and to challenge requests for access that do not appear well-founded.

SEC. 2.6. ACCESS BY NON-UNITED STATES CITIZENS.

(a) Where there are compelling reasons in furtherance of an agency mission, immigrant alien and foreign national employees who possess a special expertise may, in the discretion of the agency, be granted limited access to classified information only for specific programs, projects, contracts, licenses, certificates, or grants for which there is a need for access. Such individuals shall not be eligible for access to any greater level of classified information than the United States Government has determined may be releasable to the country of which the subject is currently a citizen, and such limited access may be approved only if the

prior 10 years of the subject's life can be appropriately investigated. If there are any doubts concerning granting access, additional lawful investigative procedures shall be fully pursued.

(b) Exceptions to these requirements may be permitted only by the agency head or the senior agency official designated under section 6.1 of this order to further substantial national security interests.

PART 3—ACCESS ELIGIBILITY STANDARDS

SEC. 3.1. STANDARDS.

(a) No employee shall be deemed to be eligible for access to classified information merely by reason of Federal service or contracting, licensee, certificate holder, or grantee status, or as a matter of right or privilege, or as a result of any particular title, rank, position, or affiliation.

(b) Except as provided in sections 2.6 and 3.3 of this order, eligibility for access to classified information shall be granted only to employees who are United States citizens for whom an appropriate investigation has been completed and whose personal and professional history affirmatively indicates loyalty to the United States, strength of character, trustworthiness, honesty, reliability, discretion, and sound judgment, as well as freedom from conflicting allegiances and potential for coercion, and willingness and ability to abide by regulations governing the use, handling, and protection of classified information. A determination of eligibility for access to such information is a discretionary security decision based on judgments by appropriately trained adjudicative personnel or appropriate automated procedures. Eligibility shall be granted only where facts and circumstances indicate access to classified information is clearly consistent with the national security interests of the United States, and any doubt shall be resolved in favor of the national security.

(c) The United States Government does not discriminate on the basis of race, color, religion, sex, national origin, disability, or sexual orientation in granting access to classified information.

(d) In determining eligibility for access under this order, agencies may investigate and consider any matter that relates to the determination of whether access is clearly consistent with the interests of national security. No inference concerning the standards in this section may be raised solely on the basis of the sexual orientation of the employee.

(e) No negative inference concerning the standards in this section may be raised solely on the basis of mental health counseling. Such counseling can be a positive factor in eligibility determinations. However, mental health counseling, where relevant to the adjudication of access to classified information, may justify further inquiry to determine whether the standards of subsection (b) of this

section are satisfied, and mental health may be considered where it directly relates to those standards.

(f) Not later than 180 days after the effective date of this order, the Security Executive Agent shall develop a common set of adjudicative guidelines for determining eligibility for access to classified information, including access to special access programs.

SEC. 3.2. BASIS FOR ELIGIBILITY APPROVAL.

(a) Eligibility determinations for access to classified information shall be based on information concerning the applicant or employee that is acquired through the investigation conducted pursuant to this order or otherwise available to security officials and shall be made part of the applicant's or employee's security record. Applicants or employees shall be required to provide relevant information pertaining to their background and character for use in investigating and adjudicating their eligibility for access.

(b) Not later than 180 days after the effective date of this order, the Security Executive Agent shall develop a common set of investigative standards for background investigations for access to classified information. These standards may vary for the various levels of access.

(c) Nothing in this order shall prohibit an agency from utilizing any lawful investigative procedure in addition to the investigative requirements set forth in this order and its implementing regulations to resolve issues that may arise during the course of a background investigation or reinvestigation.

SEC. 3.3. SPECIAL CIRCUMSTANCES.

(a) In exceptional circumstances where official functions must be performed prior to the completion of the investigative and adjudication process, temporary eligibility for access to classified information may be granted to an employee while the initial investigation is underway. When such eligibility is granted, the initial investigation shall be expedited.

(1) Temporary eligibility for access under this section shall include a justification, and the employee must be notified in writing that further access is expressly conditioned on the favorable completion of the investigation and issuance of an access eligibility approval. Access will be immediately terminated, along with any assignment requiring an access eligibility approval, if such approval is not granted.

(2) Temporary eligibility for access may be granted only by security personnel authorized by the agency head to make access eligibility determinations and shall be based on minimum investigative standards developed by the Security Executive Agent not later than 180 days after the effective date of this order.

(3) Temporary eligibility for access may be granted only to particular, identified categories of classified information necessary to perform the lawful and authorized functions that are the basis for the granting of temporary access.

(b) Nothing in subsection (a) shall be construed as altering the authority of an agency head to waive requirements for granting access to classified information pursuant to statutory authority.

(c) Where access has been terminated under section 2.1(b)(4) of this order and a new need for access arises, access eligibility up to the same level shall be reapproved without further investigation as to employees who were determined to be eligible based on a favorable adjudication of an investigation completed within the prior 5 years, provided they have remained employed by the same employer during the period in question, the employee certifies in writing that there has been no change in the relevant information provided by the employee for the last background investigation, and there is no information that would tend to indicate the employee may no longer satisfy the standards established by this order for access to classified information.

(d) Access eligibility shall be reapproved for individuals who were determined to be eligible based on a favorable adjudication of an investigation completed within the prior 5 years and who have been retired or otherwise separated from United States Government employment for not more than 2 years; provided there is no indication the individual may no longer satisfy the standards of this order, the individual certifies in writing that there has been no change in the relevant information provided by the individual for the last background investigation, and an appropriate record check reveals no unfavorable information.

SEC. 3.4. REINVESTIGATION REQUIREMENTS.

(a) Because circumstances and characteristics may change dramatically over time and thereby alter the eligibility of employees for continued access to classified information, reinvestigations shall be conducted with the same priority and care as initial investigations.

(b) Employees who are eligible for access to classified information shall be the subject of periodic reinvestigations and may also be reinvestigated if, at any time, there is reason to believe that they may no longer meet the standards for access established in this order.

(c) Not later than 180 days after the effective date of this order, the Security Executive Agent shall develop a common set of reinvestigative standards, including the frequency of reinvestigations.

SEC. 3.5. CONTINUOUS EVALUATION.

An individual who has been determined to be eligible for or who currently has access to classified information shall be subject to continuous evaluation under standards (including, but not limited to, the frequency of such evaluation) as determined by the Director of National Intelligence.

PART 4—INVESTIGATIONS FOR FOREIGN GOVERNMENTS

SEC. 4. AUTHORITY.

Agencies that conduct background investigations, including the Federal Bureau of Investigation and the Department of State, are authorized to conduct personnel security investigations in the United States when requested by a foreign government as part of its own personnel security program and with the consent of the individual.

PART 5—REVIEW OF ACCESS DETERMINATIONS

SEC. 5.1. DETERMINATIONS OF NEED FOR ACCESS.

A determination under section 2.1(b)(4) of this order that an employee does not have, or no longer has, a need for access is a discretionary determination and shall be conclusive.

SEC. 5.2. REVIEW PROCEEDINGS FOR DENIALS OR REVOCATIONS OF ELIGIBILITY FOR ACCESS.

(a) Applicants and employees who are determined to not meet the standards for access to classified information established in section 3.1 of this order shall be:

- (1) provided as comprehensive and detailed a written explanation of the basis for that conclusion as the national security interests of the United States and other applicable law permit;
- (2) provided within 30 days, upon request and to the extent the documents would be provided if requested under the Freedom of Information Act (5 U.S.C. § 552) or the Privacy Act ([5] U.S.C. § 552a), as applicable, any documents, records, and reports upon which a denial or revocation is based;
- (3) informed of their right to be represented by counsel or other representative at their own expense; to request any documents, records, and reports as described in section 5.2(a)(2) upon which a denial or revocation is based; and to request the entire investigative file, as permitted by the national security and other applicable law, which, if requested, shall be promptly provided prior to the time set for a written reply;

(4) provided a reasonable opportunity to reply in writing to, and to request a review of, the determination;

(5) provided written notice of and reasons for the results of the review, the identity of the deciding authority, and written notice of the right to appeal;

(6) provided an opportunity to appeal in writing to a high level panel, appointed by the agency head, which shall be comprised of at least three members, two of whom shall be selected from outside the security field. Decisions of the panel shall be in writing, and final except as provided in subsection (b) of this section; and

(7) provided an opportunity to appear personally and to present relevant documents, materials, and information at some point in the process before an adjudicative or other authority, other than the investigating entity, as determined by the agency head. A written summary or recording of such appearance shall be made part of the applicant's or employee's security record, unless such appearance occurs in the presence of the appeals panel described in subsection (a)(6) of this section.

(b) Nothing in this section shall prohibit an agency head from personally exercising the appeal authority in subsection (a)(6) of this section based upon recommendations from an appeals panel. In such case, the decision of the agency head shall be final.

(c) Agency heads shall promulgate regulations to implement this section and, at their sole discretion and as resources and national security considerations permit, may provide additional review proceedings beyond those required by subsection (a) of this section. This section does not require additional proceedings, however, and creates no procedural or substantive rights.

(d) When the head of an agency or principal deputy personally certifies that a procedure set forth in this section cannot be made available in a particular case without damaging the national security interests of the United States by revealing classified information, the particular procedure shall not be made available. This certification shall be conclusive.

(e) This section shall not be deemed to limit or affect the responsibility and power of an agency head pursuant to any law or other Executive order to deny or terminate access to classified information in the interests of national security. The power and responsibility to deny or terminate access to classified information pursuant to any law or other Executive order may be exercised only where the agency head determines that the procedures prescribed in subsection (a) of this section cannot be invoked in a manner that is consistent with national security. This determination shall be conclusive.

(f)(1) This section shall not be deemed to limit or affect the responsibility and power of an agency head to make determinations of suitability for employment.

(2) Nothing in this section shall require that an agency provide the procedures prescribed in subsection (a) of this section to an applicant where a conditional offer of employment is withdrawn for reasons of suitability or any other reason other than denial of eligibility for access to classified information.

(3) A suitability determination shall not be used for the purpose of denying an applicant or employee the review proceedings of this section where there has been a denial or revocation of eligibility for access to classified information.

PART 6—IMPLEMENTATION

SEC. 6.1. AGENCY IMPLEMENTING RESPONSIBILITIES.

Heads of agencies that grant employees access to classified information shall:

- (a) designate a senior agency official to direct and administer the agency's personnel security program established by this order. All such programs shall include active oversight and continuing security education and awareness programs to ensure effective implementation of this order;
- (b) cooperate, under the guidance of the Security Executive Agent, with other agencies to achieve practical, consistent, and effective adjudicative training and guidelines; and
- (c) conduct periodic evaluations of the agency's implementation and administration of this order, including the implementation of section 1.3(a) of this order. Copies of each report shall be provided to the Security Executive Agent.

SEC. 6.2. EMPLOYEE RESPONSIBILITIES.

(a) Employees who are granted eligibility for access to classified information shall:

- (1) protect classified information in their custody from unauthorized disclosure;
- (2) report all contacts with persons, including foreign nationals, who seek in any way to obtain unauthorized access to classified information;
- (3) report all violations of security regulations to the appropriate security officials; and
- (4) comply with all other security requirements set forth in this order and its implementing regulations.

(b) Employees are encouraged and expected to report any information that raises doubts as to whether another employee's continued eligibility for access to classified information is clearly consistent with the national security.

SEC. 6.3. SECURITY EXECUTIVE AGENT RESPONSIBILITIES AND IMPLEMENTATION.

(a) With respect to actions taken by the Security Executive Agent pursuant to sections 1.3(c), 3.1(f), 3.2(b), 3.3(a)(2), and 3.4(c) of this order, the Director of National Intelligence shall serve as the final authority for implementation.

(b) Any guidelines, standards, or procedures developed by the Security Executive Agent pursuant to this order shall be consistent with those guidelines issued by the Federal Bureau of Investigation in March 1994 on Background Investigations Policy/Guidelines Regarding Sexual Orientation.

(c) In carrying out its responsibilities under this order, the Security Executive Agent shall consult where appropriate with the Overseas Security Policy Board. In carrying out its responsibilities under section 1.3(c) of this order, the Security Executive Agent shall obtain the concurrence of the Director of the Office of Management and Budget.

SEC. 6.4. SANCTIONS.

Employees shall be subject to appropriate sanctions if they knowingly and willfully grant eligibility for, or allow access to, classified information in violation of this order or its implementing regulations. Sanctions may include reprimand, suspension without pay, removal, and other actions in accordance with applicable law and agency regulations.

PART 7—GENERAL PROVISIONS

SEC. 7.1. CLASSIFIED INFORMATION PROCEDURES ACT.

Nothing in this order is intended to alter the procedures established under the Classified Information Procedures Act (18 U.S.C. App. § 1).

SEC. 7.2. GENERAL.

(a) Information obtained by an agency under sections 1.2(e) or 1.3 of this order may not be disseminated outside the agency, except to:

- (1) the agency employing the employee who is the subject of the records or information;
- (2) the Department of Justice for law enforcement or counterintelligence purposes; or
- (3) any agency if such information is clearly relevant to the authorized responsibilities of such agency.

EXECUTIVE ORDER 12968, ACCESS TO CLASSIFIED INFORMATION

(b) The Attorney General, at the request of the head of an agency, shall render an interpretation of this order with respect to any question arising in the course of its administration.

(c) No prior Executive orders are repealed by this order. To the extent that this order is inconsistent with any provision of any prior Executive order, this order shall control, except that this order shall not diminish or otherwise affect the requirements of Executive Order No. 10450, the denial and revocation procedures provided to individuals covered by Executive Order No. 10865, as amended, or access by historical researchers and former presidential appointees under Executive Order No. 12958 or any successor order.

(d) If any provision of this order or the application of such provision is held to be invalid, the remainder of this order shall not be affected.

(e) This Executive order is intended only to improve the internal management of the executive branch and is not intended to, and does not, create any right to administrative or judicial review, or any other right or benefit or trust responsibility, substantive or procedural, enforceable by a party against the United States, its agencies or instrumentalities, its officers or employees, or any other person.

(f) This order is effective immediately.

-/S/-William J. Clinton
THE WHITE HOUSE,
August 2, 1995.

EXECUTIVE ORDER 13388:
FURTHER STRENGTHENING THE SHARING OF
TERRORISM INFORMATION TO PROTECT AMERICANS

[Signed: October 25, 2005, Federal Register Vol. 70, No. 207
(October 27, 2005)]

By the authority vested in me as President by the Constitution and the laws of the United States of America, including section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (Public Law 108–458), and in order to further strengthen the effective conduct of United States counterterrorism activities and protect the territory, people, and interests of the United States of America, including against terrorist attacks, it is hereby ordered as follows:

SECTION 1. POLICY. To the maximum extent consistent with applicable law, agencies shall, in the design and use of information systems and in the dissemination of information among agencies:

- (a) give the highest priority to
 - (1) the detection, prevention, disruption, preemption, and mitigation of the effects of terrorist activities against the territory, people, and interests of the United States of America;
 - (2) the interchange of terrorism information among agencies;
 - (3) the interchange of terrorism information between agencies and appropriate authorities of State, local, and tribal governments, and between agencies and appropriate private sector entities; and
 - (4) the protection of the ability of agencies to acquire additional such information; and
- (b) protect the freedom, information privacy, and other legal rights of Americans in the conduct of activities implementing subsection (a).

SEC. 2. DUTIES OF HEADS OF AGENCIES POSSESSING OR ACQUIRING TERRORISM INFORMATION. To implement the policy set forth in section 1 of this order, the head of each agency that possesses or acquires terrorism information:

- (a) shall promptly give access to the terrorism information to the head of each other agency that has counterterrorism functions, and provide the terrorism information to each such agency, unless otherwise directed by the President, and consistent with
 - (1) the statutory responsibilities of the agencies providing and receiving the information;

EXECUTIVE ORDER 13388, STRENGTHENING THE SHARING OF TERRORISM
INFORMATION

- (2) any guidance issued by the Attorney General to fulfill the policy set forth in subsection 1(b) of this order; and
- (3) other applicable law, including sections 102A(g) and (i) of the National Security Act of 1947, section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (including any policies, procedures, guidelines, rules, and standards issued pursuant thereto), sections 202 and 892 of the Homeland Security Act of 2002, Executive Order 12958 of April 17, 1995, as amended, and Executive Order 13311 of July 29, 2003; and

(b) shall cooperate in and facilitate production of reports based on terrorism information with contents and formats that permit dissemination that maximizes the utility of the information in protecting the territory, people, and interests of the United States.

SEC. 3. PREPARING TERRORISM INFORMATION FOR MAXIMUM DISTRIBUTION. To assist in expeditious and effective implementation by agencies of the policy set forth in section 1 of this order, the common standards for the sharing of terrorism information established pursuant to section 3 of Executive Order 13356 of August 27, 2004, shall be used, as appropriate, in carrying out section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004.

SEC. 4. REQUIREMENTS FOR COLLECTION OF TERRORISM INFORMATION INSIDE THE UNITED STATES. To assist in expeditious and effective implementation by agencies of the policy set forth in section 1 of this order, the recommendations regarding the establishment of executive branch-wide collection and sharing requirements, procedures, and guidelines for terrorism information collected within the United States made pursuant to section 4 of Executive Order 13356 shall be used, as appropriate, in carrying out section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004.

SEC. 5. ESTABLISHMENT AND FUNCTIONS OF INFORMATION SHARING COUNCIL.

(a) Consistent with section 1016(g) of the Intelligence Reform and Terrorism Prevention Act of 2004, there is hereby established an Information Sharing Council (Council), chaired by the Program Manager to whom section 1016 of such Act refers, and composed exclusively of designees of: the Secretaries of State, the Treasury, Defense, Commerce, Energy, and Homeland Security; the Attorney General; the Director of National Intelligence; the Director of the Central Intelligence Agency; the Director of the Office of Management and Budget; the Director of the Federal Bureau of Investigation; the Director of the

EXECUTIVE ORDER 13388, STRENGTHENING THE SHARING OF TERRORISM
INFORMATION

National Counterterrorism Center; and such other heads of departments or agencies as the Director of National Intelligence may designate.

(b) The mission of the Council is to

- (1) provide advice and information concerning the establishment of an interoperable terrorism information sharing environment to facilitate automated sharing of terrorism information among appropriate agencies to implement the policy set forth in section 1 of this order; and
- (2) perform the duties set forth in section 1016(g) of the Intelligence Reform and Terrorism Prevention Act of 2004.

(c) To assist in expeditious and effective implementation by agencies of the policy set forth in section 1 of this order, the plan for establishment of a proposed interoperable terrorism information sharing environment reported under section 5(c) of Executive Order 13356 shall be used, as appropriate, in carrying out section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004.

SEC. 6. DEFINITIONS. As used in this order:

- (a) the term “agency” has the meaning set forth for the term “executive agency” in section 105 of title 5, United States Code, together with the Department of Homeland Security, but includes the Postal Rate Commission and the United States Postal Service and excludes the Government Accountability Office; and
- (b) the term “terrorism information” has the meaning set forth for such term in section 1016(a)(4) of the Intelligence Reform and Terrorism Prevention Act of 2004.

SEC. 7. GENERAL PROVISIONS.

(a) This order:

- (1) shall be implemented in a manner consistent with applicable law, including Federal law protecting the information privacy and other legal rights of Americans, and subject to the availability of appropriations;
- (2) shall be implemented in a manner consistent with the authority of the principal officers of agencies as heads of their respective agencies, including under section 199 of the Revised Statutes (22 U.S.C. § 2651), section 201 of the Department of Energy Organization Act (42 U.S.C. § 7131), section 103 of the National Security Act of 1947 (50 U.S.C. § 403–3), section 102(a) of the Homeland Security Act of 2002 (6 U.S.C. § 112(a)), and sections 301 of title 5, 113(b) and 162(b) of title 10, 1501 of title 15, 503 of title 28, and 301(b) of title 31, United States Code;
- (3) shall be implemented consistent with the Presidential Memorandum of June 2, 2005, on “Strengthening Information Sharing, Access, and Integration—Organizational, Management, and Policy Development

EXECUTIVE ORDER 13388, STRENGTHENING THE SHARING OF TERRORISM
INFORMATION

Structures for Creating the Terrorism Information Sharing Environment;”

(4) shall not be construed to impair or otherwise affect the functions of the Director of the Office of Management and Budget relating to budget, administrative, and legislative proposals; and

(5) shall be implemented in a manner consistent with section 102A of the National Security Act of 1947.

(b) This order is intended only to improve the internal management of the Federal Government and is not intended to, and does not, create any rights or benefits, substantive or procedural, enforceable at law or in equity by a party against the United States, its departments, agencies, instrumentalities, or entities, its officers, employees, or agents, or any other person.

[SEC. 8. Amended EO 13311 and revoked EO 13356.]

-/S/-George W. Bush
THE WHITE HOUSE,
October 25, 2005.

EXECUTIVE ORDER 13462, PRESIDENT'S INTELLIGENCE ADVISORY BOARD
AND INTELLIGENCE OVERSIGHT BOARD

EXECUTIVE ORDER 13462:
PRESIDENT'S INTELLIGENCE ADVISORY BOARD AND
INTELLIGENCE OVERSIGHT BOARD

[Signed: February 29, 2008, Federal Register Vol. 73, No. 43 (March 4, 2008),
as amended by EO 13516 (2009)]

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

SECTION 1. POLICY.

It is the policy of the United States to ensure that the President and other officers of the United States with responsibility for the security of the Nation and the advancement of its interests have access to accurate, insightful, objective, and timely information concerning the capabilities, intentions, and activities of foreign powers.

SEC. 2. DEFINITIONS. As used in this order:

- (a) "department concerned" means an executive department listed in section 101 of title 5, United States Code, that contains an organization listed in or designated pursuant to section 3(4) of the National Security Act of 1947, as amended ([50 U.S.C. § 3003(4)]);
- (b) "intelligence activities" has the meaning specified in section 3.5 of Executive Order 12333 of December 4, 1981, as amended; and
- (c) "intelligence community" means the organizations listed in or designated pursuant to section 3(4) of the National Security Act of 1947, as amended.

SEC. 3. ESTABLISHMENT OF THE PRESIDENT'S INTELLIGENCE ADVISORY BOARD.

- (a) There is hereby established, within the Executive Office of the President and exclusively to advise and assist the President as set forth in this order, the President's Intelligence Advisory Board (PIAB).
- (b) The PIAB shall consist of not more than 16 members appointed by the President from among individuals who are not full-time employees of the Federal Government.
- (c) The President shall designate a Chair or Co-Chairs from among the members of the PIAB, who shall convene and preside at meetings of the PIAB, determine its agenda, and direct its work.
- (d) Members of the PIAB and the Intelligence Oversight Board (IOB) established in section 5 of this order:

EXECUTIVE ORDER 13462, PRESIDENT'S INTELLIGENCE ADVISORY BOARD
AND INTELLIGENCE OVERSIGHT BOARD

(i) shall serve without any compensation for their work on the PIAB or the IOB; and

(ii) while engaged in the work of the PIAB or the IOB, may be allowed travel expenses, including per diem in lieu of subsistence, as authorized by law for persons serving intermittently in the Government (5 U.S.C. 5701-5707).

(e) The PIAB shall utilize such full-time professional and administrative staff as authorized by the Chair and approved by the President or the President's designee. Such staff shall be supervised by an Executive Director of the PIAB, appointed by the President, whom the President may designate to serve also as the Executive Director of the IOB.

SEC. 4. FUNCTIONS OF THE PIAB. Consistent with the policy set forth in section 1 of this order, the PIAB shall have the authority to, as the PIAB determines appropriate, or shall, when directed by the President:

(a) assess the quality, quantity, and adequacy of intelligence collection, of analysis and estimates, and of counterintelligence and other intelligence activities, assess the adequacy of management, personnel and organization in the intelligence community, and review the performance of all agencies of the Federal Government that are engaged in the collection, evaluation, or production of intelligence or the execution of intelligence policy and report the results of such assessments or reviews:

(i) to the President, as necessary but not less than twice each year; and

(ii) to the Director of National Intelligence (DNI) and the heads of departments concerned when the PIAB determines appropriate; and

(b) consider and make appropriate recommendations to the President, the DNI, or the head of the department concerned with respect to matters identified to the PIAB by the DNI or the head of a department concerned.

SEC. 5. ESTABLISHMENT OF INTELLIGENCE OVERSIGHT BOARD.

(a) There is hereby established a committee of the PIAB to be known as the Intelligence Oversight Board.

(b) The IOB shall consist of not more than five members of the PIAB who are designated by the President from among members of the PIAB to serve on the IOB. The IOB shall utilize such full-time professional and administrative staff as authorized by the Chair and approved by the President or the President's designee. Such staff shall be supervised by an Executive Director of the IOB, appointed by the President, whom the President may designate to serve also as the Executive Director of the PIAB.

EXECUTIVE ORDER 13462, PRESIDENT'S INTELLIGENCE ADVISORY BOARD
AND INTELLIGENCE OVERSIGHT BOARD

(c) The President shall designate a Chair from among the members of the IOB, who shall convene and preside at meetings of the IOB, determine its agenda, and direct its work.

SEC. 6. FUNCTIONS OF THE IOB. Consistent with the policy set forth in section 1 of this order, the IOB shall:

(a) issue criteria on the thresholds for reporting matters to the IOB, to the extent consistent with section 1.6(c) of Executive Order 12333 or the corresponding provision of any successor order;

(b) inform the President of intelligence activities that the IOB believes:

(i)(A) may be unlawful or contrary to Executive Order or presidential directive; and

(B) are not being adequately addressed by the Attorney General, the DNI, or the head of the department concerned; or

(ii) should be immediately reported to the President.

(c) forward to the Attorney General information concerning intelligence activities that involve possible violations of Federal criminal laws or otherwise implicate the authority of the Attorney General;

(d) review and assess the effectiveness, efficiency, and sufficiency of the processes by which the DNI and the heads of departments concerned perform their respective functions under this order and report thereon as necessary, together with any recommendations, to the President and, as appropriate, the DNI and the head of the department concerned;

(e) receive and review information submitted by the DNI under subsection 7(c) of this order and make recommendations thereon, including for any needed corrective action, with respect to such information, and the intelligence activities to which the information relates, as necessary, but not less than twice each year, to the President, the DNI, and the head of the department concerned; and

(f) conduct, or request that the DNI or the head of the department concerned, as appropriate, carry out and report to the IOB the results of, investigations of intelligence activities that the IOB determines are necessary to enable the IOB to carry out its functions under this order.

SEC. 7. FUNCTIONS OF THE DIRECTOR OF NATIONAL INTELLIGENCE. Consistent with the policy set forth in section 1 of this order, the DNI shall:

(a) with respect to guidelines applicable to organizations within the intelligence community that concern reporting of intelligence activities described in subsection 6(b)(i)(A) of this order:

EXECUTIVE ORDER 13462, PRESIDENT'S INTELLIGENCE ADVISORY BOARD
AND INTELLIGENCE OVERSIGHT BOARD

- (i) review and ensure that such guidelines are consistent with section 1.6(c) of Executive Order 12333, or a corresponding provision of any successor order, and this order; and
 - (ii) issue for incorporation in such guidelines instructions relating to the format and schedule of such reporting as necessary to implement this order;
- (b) with respect to intelligence activities described in subsection 6(b)(i)(A) of this order:
- (i) receive reports submitted to the IOB pursuant to section 1.6(c) of Executive Order 12333, or a corresponding provision of any successor order;
 - (ii) forward to the Attorney General information in such reports relating to such intelligence activities to the extent that such activities involve possible violations of Federal criminal laws or implicate the authority of the Attorney General unless the DNI or the head of the department concerned has previously provided such information to the Attorney General; and
 - (iii) monitor the intelligence community to ensure that the head of the department concerned has directed needed corrective actions and that such actions have been taken and report to the IOB and the head of the department concerned, and as appropriate the President, when such actions have not been timely taken; and
- (c) submit to the IOB as necessary and no less than twice each year:
- (i) an analysis of the reports received under subsection (b)(i) of this section, including an assessment of the gravity, frequency, trends, and patterns of occurrences of intelligence activities described in subsection 6(b)(i)(A) of this order;
 - (ii) a summary of direction under subsection (b)(iii) of this section and any related recommendations; and
 - (iii) an assessment of the effectiveness of corrective action taken by the DNI or the head of the department concerned with respect to intelligence activities described in subsection 6(b)(i)(A) of this order.

SEC. 8. FUNCTIONS OF HEADS OF DEPARTMENTS CONCERNED AND ADDITIONAL FUNCTIONS OF THE DIRECTOR OF NATIONAL INTELLIGENCE.

- (a) To the extent permitted by law, the DNI and the heads of departments concerned shall provide such information and assistance as the PIAB and the IOB determine is needed to perform their functions under this order.

EXECUTIVE ORDER 13462, PRESIDENT'S INTELLIGENCE ADVISORY BOARD
AND INTELLIGENCE OVERSIGHT BOARD

- (b) The heads of departments concerned shall:
- (i) ensure that the DNI receives:
 - (A) copies of reports submitted to the IOB pursuant to section 1.6(c) of Executive Order 12333, or a corresponding provision of any successor order; and
 - (B) such information and assistance as the DNI may need to perform functions under this order; and
 - (ii) designate the offices within their respective organizations that shall submit reports to the IOB required by Executive Order and inform the DNI and the IOB of such designations; and
 - (iii) ensure that departments concerned comply with instructions issued by the DNI under subsection 7(a)(ii) of this order.
- (c) The head of a department concerned who does not implement a recommendation to that head of department from the PIAB under subsection 4(b) of this order or from the IOB under subsections 6(c) or 6(d) of this order shall promptly report through the DNI to the Board that made the recommendation, or to the President, the reasons for not implementing the recommendation.
- (d) The DNI shall ensure that the Director of the Central Intelligence Agency performs the functions with respect to the Central Intelligence Agency under this order that a head of a department concerned performs with respect to organizations within the intelligence community that are part of that department.

SEC. 9. REFERENCES AND TRANSITION.

- (a) References in Executive Orders other than this order, or in any other presidential guidance, to the "President's Foreign Intelligence Advisory Board" shall be deemed to be references to the President's Intelligence Advisory Board established by this order.
- (b) Individuals who are members of the President's Foreign Intelligence Advisory Board under Executive Order 12863 of September 13, 1993, as amended, immediately prior to the signing of this order shall be members of the President's Intelligence Advisory Board immediately upon the signing of this order, to serve as such consistent with this order until the date that is 15 months following the date of this order.
- (c) Individuals who are members of the Intelligence Oversight Board under Executive Order 12863 immediately prior to the signing of this order shall be members of the Intelligence Oversight Board under this order, to serve as such consistent with this order until the date that is 15 months following the date of this order.
- (d) The individual serving as Executive Director of the President's Foreign Intelligence Advisory Board immediately prior to the signing of this order shall

EXECUTIVE ORDER 13462, PRESIDENT'S INTELLIGENCE ADVISORY BOARD
AND INTELLIGENCE OVERSIGHT BOARD

serve as the Executive Director of the PIAB until such person resigns, dies, or is removed, or upon appointment of a successor under this order and shall serve as the Executive Director of the IOB until an Executive Director of the IOB is appointed or designated under this order.

SEC. 10. REVOCATION. Executive Order 12863 is revoked.

SEC. 11. GENERAL PROVISIONS.

- (a) Nothing in this order shall be construed to impair or otherwise affect:
 - (i) authority granted by law to a department or agency, or the head thereof; or
 - (ii) functions of the Director of the Office of Management and Budget relating to budget, administrative, or legislative proposals.
- (b) Any person who is a member of the PIAB or the IOB, or who is granted access to classified national security information in relation to the activities of the PIAB or the IOB, as a condition of access to such information, shall sign and comply with appropriate agreements to protect such information from unauthorized disclosure. This order shall be implemented in a manner consistent with Executive Order 12958 of April 17, 1995, as amended [revoked and replaced by EO 13526], and Executive Order 12968 of August 2, 1995, as amended.
- (c) This order shall be implemented consistent with applicable law and subject to the availability of appropriations.
- (d) This order is intended only to improve the internal management of the executive branch and is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity, by any party against the United States, its departments, agencies or entities, its officers, employees, or agents, or any other person.

-/S/- George W. Bush
THE WHITE HOUSE,
February 29, 2008.

EXECUTIVE ORDER 13467, SUITABILITY FOR GOVERNMENT EMPLOYMENT,
FITNESS FOR CONTRACTOR EMPLOYEES, AND ACCESS TO
CLASSIFIED INFORMATION

EXECUTIVE ORDER 13467:
REFORMING PROCESSES RELATED TO SUITABILITY FOR
GOVERNMENT EMPLOYMENT, FITNESS FOR CONTRACTOR
EMPLOYEES, AND ELIGIBILITY FOR ACCESS TO
CLASSIFIED NATIONAL SECURITY INFORMATION

[Signed: June 30, 2008, Federal Register Vol. 73, No. 128 (July 2, 2008),
as amended by EO 13741 (2016), EO 13764 (2017), and EO 13869 (2019)]

By the authority vested in me as President by the Constitution and the laws of the United States of America, including sections 3301, 7103(b), and 7301 of title 5, United States Code, and in order to strengthen and ensure a secure, efficient, timely, reciprocal, and aligned system for investigating and determining suitability or fitness for Government employment, fitness to work as a contractor or a nonappropriated fund employee, eligibility for access to classified information or to hold a sensitive position, and authorization to be issued a Federal credential, while providing fair, impartial, and equitable treatment, and protecting individual rights under the Constitution and laws of the United States, and taking appropriate account of title III of Public Law 108-458, it is hereby ordered as follows:

PART 1 —POLICY, APPLICABILITY, AND DEFINITIONS

SECTION 1.1. POLICY.

(a) Executive branch vetting policies and procedures relating to suitability, contractor or Federal employee fitness, eligibility to hold a sensitive position, authorization to be issued a Federal credential for access to federally controlled facilities and information systems, and eligibility for access to classified information shall be aligned using consistent standards to the extent possible, shall provide for reciprocal recognition, and shall ensure cost-effective, timely, and efficient protection of the national interest, while providing fair treatment to those upon whom the Federal Government relies to conduct our Nation's business and protect national security.

(b) The Government's tools, systems, and processes for conducting these background investigations and managing sensitive investigative information should keep pace with technological advancements, regularly integrating current best practices to better anticipate, detect, and counter malicious activities, and threats posed by external or internal actors who may seek to do harm to the

EXECUTIVE ORDER 13467, SUITABILITY FOR GOVERNMENT EMPLOYMENT,
FITNESS FOR CONTRACTOR EMPLOYEES, AND ACCESS TO
CLASSIFIED INFORMATION

Government's personnel, property, and information. To help fulfill these responsibilities, there shall be a primary executive branch investigative service provider whose mission is to provide effective, efficient, and secure background investigations for the Federal Government.

(c) Executive branch vetting policies and procedures shall be sustained by an enhanced risk-management approach that facilitates early detection of issues by an informed, aware, and responsible Federal workforce; results in quality decisions enabled by improved vetting capabilities; and advances Government-wide capabilities through enterprise approaches.

(d) The appointment or retention of each covered individual shall be subject to an investigation. Federal investigative standards established pursuant to this order shall be designed to develop information as to whether the employment or retention in employment in the Federal service of the person being investigated is clearly consistent with the interests of the national security, and the scope of the investigation shall be determined in the first instance according to the degree of material adverse effect the occupant of the position sought to be filled could bring about, by virtue of the nature of the position, on the national security.”

(e) Investigative agencies shall control the reports, information, and other investigative materials that are developed during the vetting process. Recipient departments and agencies may retain and use the received reports, information, and other investigative material within that recipient for authorized purposes (including, but not limited to, adjudications, hearings and appeals, continuous evaluation, inspector general functions, counterintelligence, research, and insider threat programs), in compliance with the Privacy Act of 1974, as amended (section 552a of title 5, United States Code). Investigative agencies shall ensure that their applicable System of Records Notices include, at a minimum, the authorized uses of the recipient departments and agencies such as those set forth above. Recipient departments and agencies shall not make any external releases of received information, other than to an investigative subject for the purpose of providing procedural rights or administrative due process; and shall direct any other requests for external releases of copies of the reports, information, and other investigative materials to the investigative agency. In the event redisclosure by the recipient agency is required by compulsory legal process, the recipient agency shall consult with the investigating agency. The investigative agency shall maintain the reports, information, and other investigative material in a system of records subject to the Privacy Act and ensure that any re-disclosure does not violate statutory restrictions or result in the unauthorized disclosure of: classified information, information subject to a claim of privilege, or information

EXECUTIVE ORDER 13467, SUITABILITY FOR GOVERNMENT EMPLOYMENT,
FITNESS FOR CONTRACTOR EMPLOYEES, AND ACCESS TO
CLASSIFIED INFORMATION

that is otherwise lawfully exempt from disclosure. Subject to Security Executive Agent authorizations consistent with section 3341(e)(5) of title 50, United States Code, the investigative agencies shall make reports, information, and other investigative material available, as necessary, to carry out the responsibilities set forth in this order, including but not limited to, authorized executive branch-sponsored research and initiatives for enterprise-wide continuous performance improvement of vetting policy and procedures, as permitted by law.

SEC. 1.2. APPLICABILITY.

(a) This order applies to vetting of all covered individuals as defined in section 1.3(h), except that:

- (i) the provisions regarding eligibility for physical access to federally controlled facilities and logical access to federally controlled information systems do not apply to individuals exempted in accordance with guidance pursuant to the Federal Information Security Management Act (title III of Public Law 107-347) and Homeland Security Presidential Directive 12 of August 27, 2004; and
- (ii) the qualification standards for enlistment, appointment, and induction into the Armed Forces pursuant to title 10, United States Code, are unaffected by this order.

(b) This order also applies to vetting for employees of agencies working in or for the legislative or judicial branches when the vetting is conducted by the executive branch.

SEC. 1.3. DEFINITIONS. For the purpose of this order:

(a) “Adjudication” means the evaluation of pertinent data in a background investigation, as well as any other available information that is relevant and reliable, to determine whether a covered individual is:

- (i) suitable for Government employment;
- (ii) eligible for logical and physical access;
- (iii) eligible for access to classified information;
- (iv) eligible to hold a sensitive position; or
- (v) fit to perform work for or on behalf of the Government as a Federal employee, contractor, or nonappropriated fund employee.

(b) “Agency” means any “Executive agency” as defined in section 105 of title 5, United States Code, including the “military departments,” as defined in section 102 of title 5, United States Code, and any other entity within the executive branch that comes into possession of classified information or has

EXECUTIVE ORDER 13467, SUITABILITY FOR GOVERNMENT EMPLOYMENT,
FITNESS FOR CONTRACTOR EMPLOYEES, AND ACCESS TO
CLASSIFIED INFORMATION

designated positions as sensitive, except such an entity headed by an officer who is not a covered individual.

(c) “Classified information” means information that has been determined pursuant to Executive Order 13526 of December 29, 2009, or a successor or predecessor order, or the Atomic Energy Act of 1954 (42 U.S.C. § 2011 *et seq.*) to require protection against unauthorized disclosure.

(d) “Continuous evaluation (CE)” means a vetting process to review the background of an individual who has been determined to be eligible for access to classified information or to hold a sensitive position at any time during the period of eligibility. CE leverages a set of automated record checks and business rules to assist in the on-going assessment of an individual’s continued eligibility. CE is intended to complement continuous vetting efforts.

(e) “Continuous performance improvement” means assessing national policy and operations, adverse events, and emerging trends and technology throughout the Government’s end-to-end vetting program. It relies on research to generate data-driven decisions and uses outcome-based measurements to adjust policy and operations.

(f) “Continuous vetting” means reviewing the background of a covered individual at any time to determine whether that individual continues to meet applicable requirements.

(g) “Contractor” means an expert or consultant (not appointed under section 3109 of title 5, United States Code) to an agency; an industrial or commercial contractor, licensee, certificate holder, or grantee of any agency, including all subcontractors; a personal services contractor; or any other category of person who performs work for or on behalf of an agency (but not a Federal employee).

(h) “Covered individual” means a person who performs, or who seeks to perform, work for or on behalf of the executive branch (*e.g.*, Federal employee, military member, or contractor), or otherwise interacts with the executive branch such that the individual must undergo vetting, but does not include:

(i) the President or (except to the extent otherwise directed by the President) employees of the President under section 105 or 107 of title 3, United States Code; or

(ii) the Vice President or (except to the extent otherwise directed by the Vice President) employees of the Vice President under section 106 of title 3 or annual legislative branch appropriations acts.

(i) “End-to-end automation” means an executive branch-wide federated system that uses automation to manage and monitor cases and maintain relevant

EXECUTIVE ORDER 13467, SUITABILITY FOR GOVERNMENT EMPLOYMENT,
FITNESS FOR CONTRACTOR EMPLOYEES, AND ACCESS TO
CLASSIFIED INFORMATION

documentation of the application (but not an employment application), investigation, adjudication, and continuous evaluation processes.

(j) “Federally controlled facilities” and “federally controlled information systems” have the meanings prescribed in guidance pursuant to the Federal Information Security Management Act (title III of Public Law 107-347) and Homeland Security Presidential Directive 12.

(k) “Fitness” means the level of character and conduct determined necessary for an individual to perform work for or on behalf of a Federal agency as an employee in the excepted service (other than a position subject to suitability), or as a “contractor employee” or a “nonappropriated fund employee” as those terms are defined in Executive Order 13488 of January 16, 2009, as amended.

(l) “Investigation” means the collection and analysis of pertinent facts and data to support a determination of whether a covered individual is, and continues to be:

- (i) eligible for access to classified information;
- (ii) eligible to hold a sensitive position;
- (iii) suitable or fit for Federal employment;
- (iv) fit to perform work for or on behalf of the Federal Government as a contractor or nonappropriated fund employee; or
- (v) authorized to be issued a Federal credential.

(m) “Logical and physical access” means access other than occasional or intermittent access to federally controlled facilities or information systems.

(n) “National Background Investigations Bureau” (NBIB) means the National Background Investigations Bureau, established within the Office of Personnel Management under section 1103(a)(3) of title 5, United States Code, or a successor entity, with responsibility for conducting effective, efficient, and secure personnel background investigations pursuant to law, rule, regulation, or Executive Order.

(o) “Sensitive position” means any position within or in support of a department or agency, the occupant of which could bring about, by virtue of the nature of the position, a material adverse effect on the national security, regardless of whether the occupant has access to classified information, and regardless of whether the occupant is an employee, a military service member, or a contractor.

(p) “Suitability” has the meaning and coverage provided in 5 CFR Part 731.

(q) “Vetting” is the process by which covered individuals undergo investigation, evaluation, and adjudication of whether they are, and remain over time, suitable or fit for Federal employment, eligible to occupy a sensitive position, eligible for access to classified information, eligible to serve as a nonappropriated fund employee or a contractor, eligible to serve in the military, or authorized to be

EXECUTIVE ORDER 13467, SUITABILITY FOR GOVERNMENT EMPLOYMENT,
FITNESS FOR CONTRACTOR EMPLOYEES, AND ACCESS TO
CLASSIFIED INFORMATION

issued a Federal credential. Vetting includes all steps in the end-to-end process, including determining need (appropriate position designation), validating need (existence of a current investigation or adjudication), collecting background information via standard forms, investigative activity, adjudication, providing administrative due process or other procedural rights, and ongoing assessments to ensure that individuals continue to meet the applicable standards for the position for which they were favorably adjudicated.

**PART 2 — VETTING ENTERPRISE, RECIPROCITY, CONTINUOUS
PERFORMANCE IMPROVEMENT, AND GOVERNANCE**

SEC. 2.1. VETTING ENTERPRISE.

(a) The executive branch-wide vetting enterprise shall use, to the greatest extent practicable, aligned and consistent vetting policies, procedures, and standards, as determined by the Council and the Executive Agents. The Executive Agents shall issue guidance to implement this provision.

(b) The aligned executive branch-wide vetting enterprise shall employ modern and consistent standards and methods, enable innovations with enterprise information technology capabilities and end-to-end automation to the extent practicable, and ensure that relevant information maintained by agencies can be accessed and shared rapidly across the executive branch, while protecting national security, protecting privacy-related information, protecting civil rights and civil liberties, ensuring resulting decisions are in the national interest and in accordance with due process requirements, and providing the Federal Government with an effective trusted workforce.

(c) The investigative and adjudicative standards for fitness shall, to the extent practicable, be consistent with the standards for suitability. The Executive Agents shall establish in Federal investigative standards the elements of the level of investigation necessary for vetting for fitness.

(d) All covered individuals shall be subject to continuous vetting under standards (including, but not limited to, the frequency of such vetting) as determined by the Security Executive Agent or the Suitability and Credentialing Executive Agent exercising its Suitability Executive Agent functions, as applicable.

(e) Vetting shall include a search of records of the Federal Bureau of Investigation, including a fingerprint-based search, and any other appropriate biometric or database searches not precluded by law.

EXECUTIVE ORDER 13467, SUITABILITY FOR GOVERNMENT EMPLOYMENT,
FITNESS FOR CONTRACTOR EMPLOYEES, AND ACCESS TO
CLASSIFIED INFORMATION

SEC. 2.2. RECIPROCITY.

Except as otherwise authorized by law or policy issued by the applicable Executive Agent, agencies shall accept background investigations and adjudications conducted by other authorized agencies unless an agency determines that a particular background investigation or adjudication does not sufficiently address the standards used by that agency in determining the fitness of its excepted service employees who cannot be noncompetitively converted to the competitive service. Except as described above and except to the extent authority to apply additional requirements is vested by statute in an agency, an agency may not establish additional investigative or adjudicative requirements (other than requirements for the conduct of a polygraph examination consistent with law, directive, or regulation) that exceed existing requirements without the approval of the Suitability and Credentialing Executive Agent exercising its Suitability Executive Agent functions or Security Executive Agent, as appropriate. Any additional requirements approved by the appropriate Executive Agent shall be limited to those that are necessary to address significant needs unique to the agency involved, to protect national security, or to satisfy a requirement imposed by law.

SEC. 2.3. CONTINUOUS PERFORMANCE IMPROVEMENT.

Executive branch vetting policies, processes, and procedures shall be supported by institutionalized enterprise-wide continuous performance improvement, which shall align with and support process improvements.

SEC. 2.4. ESTABLISHMENT AND FUNCTIONS OF PERFORMANCE ACCOUNTABILITY COUNCIL.

(a) There is hereby established a Security, Suitability, and Credentialing Performance Accountability Council (Council).

(b) The Deputy Director for Management, Office of Management and Budget, shall serve as Chair of the Council and shall have authority, direction, and control over the Council's functions. Membership on the Council shall include the Suitability and Credentialing Executive Agent, the Security Executive Agent, and the Under Secretary of Defense for Intelligence. These four officials collectively shall constitute "the Security, Suitability, and Credentialing Performance Accountability Council Principals." The Director of the Defense Counterintelligence and Security Agency shall also serve as a member of the Council. The Chair shall select a Vice Chair to act in the Chair's absence. The Chair shall have authority to designate officials from additional agencies who

EXECUTIVE ORDER 13467, SUITABILITY FOR GOVERNMENT EMPLOYMENT,
FITNESS FOR CONTRACTOR EMPLOYEES, AND ACCESS TO
CLASSIFIED INFORMATION

shall serve as members of the Council. Council membership shall be limited to Federal Government employees in leadership positions.

(c) The Council shall be accountable to the President to achieve, consistent with this order, the goals of the executive branch vetting enterprise, and is responsible for driving implementation of reform efforts and enterprise development, ensuring accountability by agencies, ensuring the Executive Agents align their respective processes, and sustaining continuous performance improvement and reform momentum.

(d) The Council shall:

- (i) ensure enterprise-wide alignment of suitability, security, credentialing, and as appropriate, fitness processes;
- (ii) hold agencies accountable for the implementation of suitability, security, fitness, and credentialing processes and procedures;
- (iii) define requirements for enterprise-wide reciprocity management information technology, and develop standards for enterprise-wide information technology;
- (iv) work with agencies to implement continuous performance improvement programs, policies, and procedures; establish annual goals and progress metrics; and prepare annual reports on results;
- (v) ensure and oversee the development of tools and techniques for enhancing background investigations and adjudications;
- (vi) enable discussion and consensus resolution of differences in processes, policies, and procedures among the Council Principals, and other agencies as appropriate;
- (vii) share best practices;
- (viii) advise the Executive Agents on policies affecting the alignment of investigations and adjudications;
- (ix) work with agencies to develop agency policies and procedures to enable sharing of vetting information consistent with the law and the protection of privacy and civil liberties and to the extent necessary for enterprise-wide efficiency, effectiveness, and security;
- (x) monitor performance to identify and drive enterprise-level process enhancements, and make recommendations for changes to executive branch-wide guidance and authorities to resolve overlaps or close policy gaps where they may exist;
- (xi) promote data-driven, transparent, and expeditious policy-making processes; and

EXECUTIVE ORDER 13467, SUITABILITY FOR GOVERNMENT EMPLOYMENT,
FITNESS FOR CONTRACTOR EMPLOYEES, AND ACCESS TO
CLASSIFIED INFORMATION

(xii) develop and continuously reevaluate and revise outcome-based metrics that measure the quality, efficiency and effectiveness of the vetting enterprise.

(e) The Chair shall, to further the goals of the vetting enterprise and to the extent consistent with law, establish subordinate entities, mechanisms, and policies to support and assist in exercising the Council's authorities and responsibilities, and facilitate, consistent with the executive branch's enterprise strategy, adoption of enterprise-wide standards and solutions to ensure security, quality, reciprocity, efficiency, effectiveness, and timeliness. The Chair may assign, in whole or in part, to the head of any agency (solely or jointly) any function within the Council's authority or responsibilities pursuant to this order.

SEC. 2.5. ESTABLISHMENT, DESIGNATION, AND FUNCTIONS OF EXECUTIVE AGENTS.

(a) There are hereby established a Suitability and Credentialing Executive Agent and a Security Executive Agent.

(b) The Director of the Office of Personnel Management shall serve as the Suitability and Credentialing Executive Agent. With respect to the Suitability Executive Agent functions, the Director:

(i) shall, pursuant to sections 1103 and 1104 of title 5, United States Code, and the Civil Service Rules, be responsible for suitability and fitness by prescribing suitability standards and minimum standards of fitness for employment; prescribing position designation requirements with regard to the risk to the efficiency and integrity of the service; prescribing applicable investigative standards, policies, and procedures for suitability and fitness; prescribing suitability and fitness reciprocity standards; making suitability determinations; and taking suitability actions;

(ii) shall issue regulations, guidance, and standards to fulfill the Director's responsibilities related to suitability and fitness under Executive Order 13488 of January 16, 2009, as amended;

(iii) shall promote reciprocal recognition of suitability or fitness determinations among the agencies, including acting as the final authority to arbitrate and resolve disputes among the agencies involving the reciprocity of investigations and adjudications of suitability and fitness;

(iv) shall continue to initially approve, and periodically review for renewal, agencies' requests to administer polygraphs in connection with

EXECUTIVE ORDER 13467, SUITABILITY FOR GOVERNMENT EMPLOYMENT,
FITNESS FOR CONTRACTOR EMPLOYEES, AND ACCESS TO
CLASSIFIED INFORMATION

appointment in the competitive service, in consultation with the Security Executive Agent as appropriate;

(v) shall make a continuing review of agency programs for suitability and fitness vetting to determine whether they are being implemented according to this order;

(vi) may issue guidelines and instructions to the heads of agencies to promote appropriate uniformity, centralization, efficiency, effectiveness, reciprocity, timeliness, and security in processes relating to determining suitability or fitness; and

(vii) shall, pursuant to section 1104 of title 5, United States Code, prescribe performance standards and a system of oversight for any suitability or fitness function delegated by the Director to the head of another agency, including uniform and consistent policies and procedures to ensure the effective, efficient, timely, and secure completion of delegated functions.

(c) With respect to the Credentialing Executive Agent functions, the Director of the Office of Personnel Management:

(i) shall develop standards for investigations, reinvestigations, and continuous vetting for a covered individual's eligibility for a personal identity verification credential permitting logical and physical access to federally controlled facilities and federally controlled information systems (PIV credential);

(ii) shall develop adjudicative guidelines for a covered individual's eligibility for a PIV credential;

(iii) shall develop guidelines on reporting and recording determinations of eligibility for a PIV credential;

(iv) shall develop standards for unfavorable determinations of eligibility for a PIV credential, including procedures for denying and revoking the eligibility for a PIV credential, for reconsideration of unfavorable determinations, and for rendering the PIV credential inoperable;

(v) shall develop standards and procedures for suspending eligibility for a PIV credential when there is a reasonable basis to believe there may be an unacceptable risk pending an inquiry or investigation, including special standards and procedures for imminent risk;

(vi) shall be responsible for developing uniform and consistent policies and procedures to ensure the effective, efficient, timely, and secure completion of investigations and adjudications relating to eligibility for a PIV credential;

EXECUTIVE ORDER 13467, SUITABILITY FOR GOVERNMENT EMPLOYMENT,
FITNESS FOR CONTRACTOR EMPLOYEES, AND ACCESS TO
CLASSIFIED INFORMATION

(vii) may develop guidelines and instructions to the heads of agencies as necessary to ensure appropriate uniformity, centralization, efficiency, effectiveness, and timeliness in processes relating to eligibility for a PIV credential;

(viii) shall monitor and make a continuing review of agency programs for determining eligibility for a PIV credential to determine whether they are being implemented according to this order; and

(ix) shall consult to the extent practicable with other agencies with responsibilities related to PIV credentials to ensure that policies and procedures are consistent with law including:

(A) the Office of Management and Budget, in exercising its responsibilities under section 11331 of title 40, United States Code, section 3553(a) of title 44, United States Code, division A, sections 1086(b)(2) and (b)(3) of Public Law 114-92, and Homeland Security Presidential Directive 12 of August 27, 2004;

(B) the Department of Homeland Security, in exercising its responsibilities under sections 3553(b), (f), and (g) of title 44, United States Code;

(C) the Department of Defense, in exercising its responsibilities under section 3553(e) of title 44, United States Code, and division A, sections 1086(a)(1)(E), (b)(1), and (b)(2) of Public Law 114-92;

(D) the Office of the Director of National Intelligence, in exercising its responsibilities under section 3553(e) of title 44, United States Code, and division A, section 1086(b)(2) of Public Law 114-92;

(E) the Department of Commerce and the National Institute of Standards and Technology, in exercising their responsibilities under section 278g-3 of title 15, United States Code, and Homeland Security Presidential Directive 12 of August 27, 2004;

(F) the General Services Administration, in exercising its responsibilities under division A, section 1086(b)(2) of Public Law 114-92; and

(G) the Federal Acquisition Regulation agencies, in exercising their responsibilities under chapter 137 of title 10, section 121(c) of title 40, and section 20113 of title 51, United States Code.

EXECUTIVE ORDER 13467, SUITABILITY FOR GOVERNMENT EMPLOYMENT,
FITNESS FOR CONTRACTOR EMPLOYEES, AND ACCESS TO
CLASSIFIED INFORMATION

(d) In fulfilling the Credentialing Executive Agent function of developing policies and procedures for determining eligibility for a PIV credential and to protect the national security, the Director of the Office of Personnel Management shall coordinate with and obtain the concurrence of the other Council Principals. Agencies with authority to establish standards or guidelines or issue instructions related to PIV credentials shall retain the discretion as to whether to establish policies, guidelines, or instructions developed by the Credentialing Executive Agent.

(e) The Director of National Intelligence shall serve as the Security Executive Agent. The Security Executive Agent:

- (i) shall direct the oversight of investigations, reinvestigations, adjudications, and, as applicable, polygraphs for eligibility for access to classified information or eligibility to hold a sensitive position made by any agency;
- (ii) shall make a continuing review of agencies' national security background investigation and adjudication programs to determine whether they are being implemented according to this order;
- (iii) shall be responsible for developing and issuing uniform and consistent policies and procedures to ensure the effective, efficient, timely, and secure completion of investigations, polygraphs, and adjudications relating to determinations of eligibility for access to classified information or eligibility to hold a sensitive position;
- (iv) may issue guidelines and instructions to the heads of agencies to ensure appropriate uniformity, centralization, efficiency, effectiveness, timeliness, and security in processes relating to determinations by agencies of eligibility for access to classified information or eligibility to hold a sensitive position, to include such matters as investigations, polygraphs, adjudications, and reciprocity;
- (v) may, if consistent with the national security, authorize exceptions to or waivers of national security investigative requirements, and may issue implementing or clarifying guidance as necessary;
- (vi) shall serve as the final authority to designate an agency or agencies, to the extent that it is not practicable to use the Defense Counterintelligence and Security Agency, to conduct investigations of persons who are proposed for access to classified information or for eligibility to hold a sensitive position to ascertain whether such persons satisfy the criteria for obtaining and retaining access to classified information or eligibility to hold a sensitive position;

EXECUTIVE ORDER 13467, SUITABILITY FOR GOVERNMENT EMPLOYMENT,
FITNESS FOR CONTRACTOR EMPLOYEES, AND ACCESS TO
CLASSIFIED INFORMATION

(vii) shall serve as the final authority to designate an agency or agencies to determine eligibility for access to classified information or eligibility to hold a sensitive position in accordance with Executive Order 12968 of August 2, 1995, as amended;

(viii) shall ensure reciprocal recognition of eligibility for access to classified information or eligibility to hold a sensitive position among the agencies, including acting as the final authority to arbitrate and resolve disputes among the agencies involving the reciprocity of investigations and adjudications of eligibility; and

(ix) may assign, in whole or in part, to the head of any agency (solely or jointly) any of the functions detailed in (i) through (viii) of this subsection, with the agency's exercise of such assigned functions to be subject to the Security Executive Agent's oversight and with such terms and conditions (including approval by the Security Executive Agent) as the Security Executive Agent determines appropriate.

(f) Nothing in this section shall be construed in a manner that would limit the authorities of the Director of the Office of Personnel Management, the Director of National Intelligence, or the Secretary of Defense under law.

SEC. 2.6. ROLES AND RESPONSIBILITIES OF THE DEPARTMENT OF DEFENSE, THE OFFICE OF PERSONNEL MANAGEMENT, AND THE OFFICE OF MANAGEMENT AND BUDGET.

(a) The National Background Investigations Bureau shall, until such functions are transferred or delegated, as applicable, to the Defense Counterintelligence and Security Agency:

- (i) serve as the primary executive branch service provider for background investigations for eligibility for access to classified information; eligibility to hold a sensitive position; suitability or, for employees in positions not subject to suitability, fitness for Government employment; fitness to perform work for or on behalf of the Government as a contractor; fitness to work as a nonappropriated fund employee, as defined in Executive Order 13488 of January 16, 2009, as amended; and authorization to be issued a Federal credential for logical and physical access to federally controlled facilities or information systems;
- (ii) provide effective, efficient, and secure personnel background investigations for the Federal Government;
- (iii) provide the Council information, to the extent permitted by law, on matters of performance, timeliness, capacity, information technology

EXECUTIVE ORDER 13467, SUITABILITY FOR GOVERNMENT EMPLOYMENT,
FITNESS FOR CONTRACTOR EMPLOYEES, AND ACCESS TO
CLASSIFIED INFORMATION

modernization, continuous performance improvement, and other relevant aspects of NBIB operations;

(iv) be headquartered in or near Washington, District of Columbia;

(v) have dedicated resources, including but not limited to a senior privacy and civil liberties official;

(vi) institutionalize interagency collaboration and leverage expertise across the executive branch;

(vii) continuously improve investigative operations, emphasizing information accuracy and protection, and regularly integrate best practices, including those identified by subject matter experts from industry, academia, or other relevant sources;

(viii) conduct personnel background investigations in accordance with uniform and consistent policies, procedures, standards, and requirements established by the Security Executive Agent and the Suitability and Credentialing Executive Agent exercising its Suitability Executive Agent functions; and

(ix) conduct other personnel background investigations as authorized by law, rule, regulation, or Executive Order;

except that throughout the transition period ending on or before September 30, 2019, as described in sections 2.6(d)(vi) and 2.6(e)(viii) of this order, the National Background Investigations Bureau and its personnel may continue to perform background investigations for the Defense Counterintelligence and Security Agency.

(b) The Secretary of Defense shall design, develop, deploy, operate, secure, defend, and continuously update and modernize, as necessary, vetting information technology systems that support all background investigation processes conducted by the National Background Investigations Bureau. Design and operation of the information technology systems for the National Background Investigations Bureau shall comply with applicable information technology standards and, to the extent practicable, ensure security and interoperability with other background investigation information technology systems. The Secretary of Defense shall operate the database in the information technology systems containing appropriate data relevant to the granting, denial, or revocation of eligibility for access to classified information or eligibility for a sensitive position pertaining to military, civilian, or Government contractor personnel, see section 3341(e) of title 50, United States Code, consistent with and following an explicit delegation from the Director of the Office of Personnel Management pursuant to section 1104 of title 5, United States Code.

EXECUTIVE ORDER 13467, SUITABILITY FOR GOVERNMENT EMPLOYMENT,
FITNESS FOR CONTRACTOR EMPLOYEES, AND ACCESS TO
CLASSIFIED INFORMATION

(i) Pursuant to sections 113 and 191 of title 10, United States Code, the Secretary of Defense shall rename the Defense Security Service (DSS) as the Defense Counterintelligence and Security Agency (DCSA). Subject to the authority, direction, and control of the Secretary of Defense and as further described in subsections (b)(ii) through (b)(iv) of this section, the DCSA shall serve as the primary Federal entity for conducting background investigations for the Federal Government. The DCSA shall, as a continuation of the former DSS, serve as the primary Department of Defense component for the National Industrial Security Program and shall execute responsibilities relating to continuous vetting, insider threat programs, and any other responsibilities assigned to it by the Secretary of Defense consistent with law. The Secretary of Defense may rename the DCSA and reassign any of its responsibilities to another Department of Defense component or components, provided, however, that the Secretary of Defense shall consult with the Directors of National Intelligence, the Office of Personnel Management, and the Office of Management and Budget before renaming the DCSA or reassigning the responsibilities specified in section 2.6(b)(ii) and (iv) of this order to another Department of Defense component.

(ii) Pursuant to and consistent with section 3001(c) of the Intelligence Reform and Terrorism Prevention Act of 2004 (50 U.S.C. § 3341(c)), sections 925(a)(1) and (d)(2) of the National Defense Authorization Act for Fiscal Year 2018 (10 U.S.C. § 1564 note), and in accordance with subsection (d) of this section, no later than June 24, 2019, the DCSA shall serve as the primary entity for conducting effective, efficient, and secure background investigations for the Federal Government for determining whether covered individuals are or continue to be eligible for access to classified information or eligible to hold a sensitive position.

(iii) Pursuant to and consistent with sections 925(a)(1) and (d)(2) of the National Defense Authorization Act for Fiscal Year 2018 (10 U.S.C. § 1564 note) and in accordance with subsection (d) of this section, no later than June 24, 2019, the DCSA shall serve as the primary entity for conducting effective, efficient, and secure background investigations for determining the suitability or, for employees in positions not subject to suitability, fitness for Department of Defense employment; fitness to perform work for or on behalf of the Department of Defense as a contractor; fitness to work as a nonappropriated fund employee, as

EXECUTIVE ORDER 13467, SUITABILITY FOR GOVERNMENT EMPLOYMENT,
FITNESS FOR CONTRACTOR EMPLOYEES, AND ACCESS TO
CLASSIFIED INFORMATION

defined in Executive Order 13488 of January 16, 2009, as amended; and authorization to be issued a Federal credential for logical and physical access to facilities or information systems controlled by the Department of Defense.

(iv) Consistent with and following an explicit delegation from the Director of the Office of Personnel Management pursuant to section 1104 of title 5, United States Code, and consistent with subsection (e) of this section, no later than June 24, 2019, the DCSA shall serve as the primary entity for conducting effective, efficient, and secure background investigations for the Federal Government not described in subsections (b)(ii) and (b)(iii) of this section, for determining suitability or, for employees in positions not subject to suitability, fitness for Government employment; fitness to perform work for or on behalf of the Government as a contractor; fitness to work as a nonappropriated fund employee, as defined in Executive Order 13488 of January 16, 2009, as amended; and authorization to be issued a Federal credential for logical and physical access to federally controlled facilities or information systems.

(v) The DCSA shall conduct other background investigations as authorized by law, designation, rule, regulation, or Executive Order.

(vi) The DCSA shall provide information to the Council established by section 2.4 of this order regarding matters of performance, including timeliness and continuous improvement, capacity, information technology modernization, and other relevant aspects of its operations. The DCSA shall be subject to the oversight of the Security Executive Agent, including implementation of Security Executive Agent policies, procedures, guidance, and instructions, in conducting investigations for eligibility to access classified information or to hold a sensitive position. The DCSA, through the Secretary of Defense, also shall be subject to the oversight of the Suitability and Credentialing Executive Agent, including implementation of Suitability and Credentialing Executive Agent policies, procedures, guidance, and instructions, and applicable Office of Personnel Management regulations, in conducting investigations of suitability or fitness and eligibility for logical and physical access.

(vii) The Secretary of Defense shall design, develop, deploy, operate, secure, defend, and continuously update and modernize, as necessary, information technology systems that support all personnel vetting processes conducted by the Department of Defense. Design and operation of these information technology systems shall comply with

EXECUTIVE ORDER 13467, SUITABILITY FOR GOVERNMENT EMPLOYMENT,
FITNESS FOR CONTRACTOR EMPLOYEES, AND ACCESS TO
CLASSIFIED INFORMATION

applicable information technology standards and, to the extent practicable, ensure security and interoperability with other personnel vetting or related information technology systems. The Secretary of Defense shall maintain and safeguard the information relevant to the granting, denial, or revocation of eligibility for access to classified information, or eligibility for a sensitive position, or relevant to suitability, fitness, or credentialing determinations pertaining to military, civilian, or Government contractor personnel. The Secretary of Defense shall operate the database in the information technology systems containing appropriate data relevant to the granting, denial, or revocation of eligibility for access to classified information or eligibility for a sensitive position pertaining to military, civilian, or Government contractor personnel, see section 3341(e) of title 50, United States Code, consistent with, as applicable, an explicit delegation from the Director of the Office of Personnel Management pursuant to section 1104 of title 5, United States Code.

(viii) The Secretary of Defense shall, by June 24, 2019, execute a written agreement with the Director of the Office of Personnel Management designating the appropriate support functions to be transferred as part of the investigative mission, consistent with section 925(d)(2)(B) of the National Defense Authorization Act for Fiscal Year 2018 (10 U.S.C. § 1564 note), and setting forth expectations for the transition period, including for detailing personnel, funding background investigations, using and safeguarding information technology, managing facilities and property, contracting, administrative support, records access, and addressing any claims.

(ix) The Secretary of Defense shall, upon finalization of the agreement described in paragraph (viii) of this subsection and in accordance with its terms:

(A) establish the Personnel Vetting Transformation Office within the Department of Defense, which will include personnel from the Department of Defense and other stakeholder agencies, as appropriate; and

(B) commence efforts to receive transferred or delegated functions and, as appropriate, associated Office of Personnel Management operations, resources, and personnel, to the DCSA.

EXECUTIVE ORDER 13467, SUITABILITY FOR GOVERNMENT EMPLOYMENT,
FITNESS FOR CONTRACTOR EMPLOYEES, AND ACCESS TO
CLASSIFIED INFORMATION

- (x) The Secretary of Defense shall:
- (A) no later than June 24, 2019, and every 180 days thereafter until the transfer is complete, provide a report to the President, in coordination with the Director of the Office of Personnel Management and through the Director of the Office of Management and Budget, regarding the status of the transfer, including any resource or funding shortfall and gaps in authority;
 - (B) take necessary actions to enable the Department of Defense to receive any resources, including personnel, made available as a result of subsection (d) of this section; and
 - (C) notify the President upon completion of the transition period.
- (xi) In the event the agreement described in paragraph (viii) of this subsection and section 2.6(e)(v) of this order is not executed by June 24, 2019, beginning on such date, the Secretary of Defense shall begin to take necessary actions to begin execution of paragraph (ix) until the agreement described in paragraph (viii) of this subsection is executed, at which time the Secretary of Defense shall ensure actions subject to such agreement under paragraph (ix) of this subsection are executed in accordance with its terms.

(c) Existing delegations of authority to conduct background investigations made by the Director of the Office of Personnel Management, as the Suitability and Credentialing Executive Agent or as otherwise authorized by statute or Executive Order, to any agency relating to suitability, fitness, or credentialing determinations, existing designations made by the Director of National Intelligence, as the Security Executive Agent or as otherwise authorized by statute or Executive Order, relating to investigating persons who are proposed for access to classified information or for eligibility to hold a sensitive position, or existing delegations of authority to conduct background investigations made by the President to any other agency through any Executive Order shall remain in effect. Nothing in this order shall be construed to limit the authority of any agency to conduct its own background investigations when specifically authorized or directed to do so by statute or any preexisting delegation from the President.

(d) Consistent with section 3503 of title 5, United States Code, subchapter I of chapter 83 of title 10, United States Code, and section 925(d)(1) of the National Defense Authorization Act for Fiscal Year 2018 (10 U.S.C. § 1564 note), the Secretary of Defense and the Director of the Office of Personnel Management, in consultation with the Director of the Office of Management and Budget and the

EXECUTIVE ORDER 13467, SUITABILITY FOR GOVERNMENT EMPLOYMENT,
FITNESS FOR CONTRACTOR EMPLOYEES, AND ACCESS TO
CLASSIFIED INFORMATION

Security Executive Agent, shall, consistent with applicable law, provide for the transfer of the functions described in sections 2.6(b)(ii) and (iii) of this order from the Office of Personnel Management's NBIB to DCSA, and any appropriate Office of Personnel Management-associated personnel and resources, including infrastructure and the investigation-related support functions. The transfer shall commence no later than June 24, 2019, and shall:

- (i) be executed with the assistance of the Personnel Vetting Transformation Office established pursuant to paragraph (b)(ix) of this section, which shall, in providing such assistance, consider input from other stakeholder agencies, as appropriate;
 - (ii) be conducted in accordance with a risk management approach that is consistent with Office of Management and Budget Circular A-123;
 - (iii) include any appropriate funds that the Secretary of Defense and the Director of the Office of Personnel Management, with the concurrence of the Director of the Office of Management and Budget, determine to be available and necessary to finance and discharge the functions transferred;
 - (iv) be consistent with the transition from legacy information technology as required by subsection (b)(vii) of this section;
 - (v) build upon the implementation plan developed pursuant to section 951(a)(1) of the National Defense Authorization Act for Fiscal Year 2017 (Public Law 114-328), which is being implemented pursuant to section 925 of the National Defense Authorization Act for Fiscal Year 2018 (10 U.S.C. § 1564 note); and
 - (vi) permit NBIB to conduct background investigations for DCSA, as necessary, until September 30, 2019.
- (e) The Director of the Office of Personnel Management shall:
- (i) no later than June 24, 2019, take any steps necessary to make effective the delegation, pursuant to section 1104(a)(2) of title 5, United States Code, of the functions described in subsection (b)(iv) of this section;
 - (ii) promptly establish appropriate performance standards and oversight as required by section 1104(b) of title 5, United States Code;
 - (iii) work in coordination with the Secretary of Defense to reassign appropriate resources, including personnel, to the DCSA and provide all necessary and appropriate support to the DCSA in a timely manner to enable it to fulfill its responsibilities under this order;

EXECUTIVE ORDER 13467, SUITABILITY FOR GOVERNMENT EMPLOYMENT,
FITNESS FOR CONTRACTOR EMPLOYEES, AND ACCESS TO
CLASSIFIED INFORMATION

- (iv) no later than June 24, 2019, provide the Secretary of Defense with a complete inventory of NBIB personnel, resources, and assets, and other Office of Personnel Management personnel and resources that primarily support NBIB;
- (v) no later than June 24, 2019, execute a written agreement with the Secretary of Defense designating the appropriate support functions to be transferred as part of the investigative mission, consistent with section 925(d)(2)(B) of the National Defense Authorization Act for Fiscal Year 2018 (10 U.S.C. § 1564 note), as described in section 2.6(b)(viii) of this order;
- (vi) immediately upon the finalization of the agreement described in paragraph (v) of this subsection and section 2.6(b)(viii) of this order, commence efforts to transition transferred or delegated functions and, as appropriate, associated Office of Personnel Management authorities, operations, resources, and personnel, to the DCSA;
- (vii) during the transition period, coordinate with the Department of Defense regarding any decisions concerning NBIB's personnel structure, finances, contracts, or organization to the extent provided in the written agreement described by paragraph (b)(viii) of this section;
- (viii) no later than September 30, 2019, complete the transfer of all designated administrative and operational functions to the Department of Defense and revoke any applicable delegation or designation to NBIB of investigative or other authority; and
- (ix) in the event the agreement described in paragraph (v) of this subsection and section 2.6(b)(viii) of this order is not executed by June 24, 2019, beginning on such date, the Director of the Office of Personnel Management shall begin to take necessary actions to begin execution of paragraphs (iii) through (viii) of this subsection until the agreement described in paragraph (v) of this subsection and section 2.6(b)(viii) of this order is executed, at which time the Director of the Office of Personnel Management shall ensure actions subject to such agreement under paragraphs (iii) through (viii) of this subsection are executed in accordance with its terms.

(f) The Director of the Office of Management and Budget shall:

- (i) facilitate an effective transfer of functions, including personnel and resources;
- (ii) support the Department of Defense's efforts to establish a single, centralized funding capability for its background investigations, as

EXECUTIVE ORDER 13467, SUITABILITY FOR GOVERNMENT EMPLOYMENT,
FITNESS FOR CONTRACTOR EMPLOYEES, AND ACCESS TO
CLASSIFIED INFORMATION

- required by section 925(e)(1) of the National Defense Authorization Act for Fiscal Year 2018 (10 U.S.C. § 1564 note);
- (iii) mediate any disagreements between the Secretary of Defense and the Director of the Office of Personnel Management that may arise during or outside of the transition period and facilitate resolution of the conflicting positions; and
 - (iv) develop, in consultation with the Secretary of Defense and the Director of the Office of Personnel Management, an appropriate funding plan for the activities undertaken pursuant to this order.

SEC. 2.7. ADDITIONAL FUNCTIONS.

(a) The duties assigned to the Security Policy Board by Executive Order 12968 of August 2, 1995, to consider, coordinate, and recommend policy directives for executive branch security policies, procedures, and practices are reassigned to the Security Executive Agent.

(b) Heads of agencies shall:

- (i) designate, or cause to be designated, as a “sensitive position,” any position occupied by a covered individual in which the occupant could bring about by virtue of the nature of the position, a material adverse effect on the national security;
- (ii) establish and maintain within their respective agencies, an effective program to ensure that employment and retention of any covered individual within the agency is clearly consistent with the interests of national security and, as applicable, meets standards for eligibility for access to classified information or to hold a sensitive position, suitability, fitness, or credentialing, established by the respective Executive Agent;
- (iii) carry out any function assigned to the agency head by the Chair, and shall assist the Chair, the Council, the Executive Agents, the National Background Investigations Bureau, and the Department of Defense in carrying out any function under sections 2.4, 2.5, and 2.6 of this order;
- (iv) implement any policy or procedure established pursuant to this order;
- (v) to the extent permitted by law, make available to the Council, the Executive Agents, the National Background Investigations Bureau, and the Department of Defense such information as may be requested to implement this order, including information necessary to implement enterprise-wide vetting policies and procedures;

EXECUTIVE ORDER 13467, SUITABILITY FOR GOVERNMENT EMPLOYMENT,
FITNESS FOR CONTRACTOR EMPLOYEES, AND ACCESS TO
CLASSIFIED INFORMATION

(vi) except as authorized by section 3341(e)(5) of title 50, United States Code, promptly furnish, or cause to be promptly furnished, to the Office of Personnel Management the information deemed by the Executive Agents to be necessary for purposes of record keeping and reciprocity including, but not limited to, the date on which a background investigation is initiated, the date on which the background investigation is closed, and the specific adjudicative or access decision made. The Executive Agents shall determine the appropriate timeline pursuant to which this information must be reported to the Office of Personnel Management. The Executive Agents shall maintain discretion to determine the scope of information needed for record keeping and reciprocity purposes. The Office of Personnel Management shall regularly provide this information to the Director of National Intelligence for national security purposes.

(vii) ensure that all actions taken under this order take account of the counterintelligence interests of the United States, as appropriate; and

(viii) ensure that actions taken under this order are consistent with the President's constitutional authority to:

(A) conduct the foreign affairs of the United States;

(B) withhold information the disclosure of which could impair the foreign relations, the national security, the deliberative processes of the Executive, or the performance of the Executive's constitutional duties;

(C) recommend for congressional consideration such measures as the President may judge necessary or expedient; and

(D) supervise the unitary executive branch.

(c) All investigations being conducted by agencies that develop information indicating that an individual may have been subjected to coercion, influence, or pressure to act contrary to the interests of the national security, or information that the individual may pose a counterintelligence or terrorist threat, or as otherwise provided by law, shall be referred to the Federal Bureau of Investigation for potential investigation, and may also be referred to other agencies where appropriate.

EXECUTIVE ORDER 13467, SUITABILITY FOR GOVERNMENT EMPLOYMENT,
FITNESS FOR CONTRACTOR EMPLOYEES, AND ACCESS TO
CLASSIFIED INFORMATION

PART 3 – MISCELLANEOUS

SEC. 3. GENERAL PROVISIONS.

(a) Executive Order 13381 of June 27, 2005, as amended, and Executive Order 10450 of April 27, 1953, as amended, are revoked. By revoking Executive Order 10450 of April 27, 1953, as amended, there is no intent to alter the requirement for an investigation for national security purposes or the “clearly consistent with the interest of national security” standard prescribed by that Executive Order for making the determinations referenced in section 2.7(b)(ii). Further, suitability, fitness, credentialing, and national security eligibility regulations, standards and guidance issued by, or interagency agreements entered into by, the Council, the Executive Agents, or any agency pursuant to Executive Order 10450 of April 27, 1953, as amended, shall remain valid until superseded. Nothing in this order shall:

- (i) supersede, impede, or otherwise affect:
 - (A) Executive Order 10577 of November 23, 1954, as amended;
 - (B) Executive Order 12333 of December 4, 1981, as amended;
 - (C) Executive Order 12829 of January 6, 1993, as amended; or
 - (D) Executive Order 13526 of December 29, 2009; nor
- (ii) diminish or otherwise affect the denial and revocation procedures provided to individuals covered by Executive Order 10865 of February 20, 1960, as amended; or
- (iii) be applied in such a way as to affect any administrative proceeding pending on the date of this order.

(b) [Amended EO 12968.]

(c) Provisions of Executive Order 12968 of August 2, 1995, as amended, that apply to eligibility for access to classified information shall apply to eligibility to hold any sensitive position regardless of whether that sensitive position requires access to classified information, subject to the Security Executive Agent issuing implementing or clarifying guidance regarding requirements for sensitive positions. Nothing in this order shall supersede, impede, or otherwise affect the remainder of Executive Order 12968 of August 2, 1995, as amended.

(d) Nothing in this order shall be construed to impair or otherwise affect the:

- (i) authority granted by law to a department or agency, or the head thereof; or
- (ii) functions of the Director of the Office of Management and Budget relating to budgetary, administrative, or legislative proposals.

EXECUTIVE ORDER 13467, SUITABILITY FOR GOVERNMENT EMPLOYMENT,
FITNESS FOR CONTRACTOR EMPLOYEES, AND ACCESS TO
CLASSIFIED INFORMATION

(e) This order shall be implemented consistent with applicable law and subject to the availability of appropriations.

(f) Existing delegations of authority made pursuant to Executive Order 13381 of June 27, 2005, as amended, to any agency relating to granting eligibility for access to classified information shall remain in effect, subject to the exercise of authorities pursuant to this order to revise or revoke such delegation.

(g) Existing delegations of authority made by the Office of Personnel Management to any agency relating to suitability or fitness shall remain in effect, subject to the exercise of authorities to revise or revoke such delegations.

(h) If any provision of this order or the application of such provision is held to be invalid, the remainder of this order shall not be affected.

(i) This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

-/S/- George W. Bush
THE WHITE HOUSE,
June 30, 2008.

EXECUTIVE ORDER 13491:
ENSURING LAWFUL INTERROGATION

[Signed: January 22, 2009, Federal Register Vol. 74, No. 16 (January 27, 2009)]

By the authority vested in me by the Constitution and the laws of the United States of America, in order to improve the effectiveness of human intelligence gathering, to promote the safe, lawful, and humane treatment of individuals in United States custody and of United States personnel who are detained in armed conflicts, to ensure compliance with the treaty obligations of the United States, including the Geneva Conventions, and to take care that the laws of the United States are faithfully executed, I hereby order as follows:

SECTION 1. REVOCATION. Executive Order 13440 of July 20, 2007, is revoked. All executive directives, orders, and regulations inconsistent with this order, including but not limited to those issued to or by the Central Intelligence Agency (CIA) from September 11, 2001, to January 20, 2009, concerning detention or the interrogation of detained individuals, are revoked to the extent of their inconsistency with this order. Heads of departments and agencies shall take all necessary steps to ensure that all directives, orders, and regulations of their respective departments or agencies are consistent with this order. Upon request, the Attorney General shall provide guidance about which directives, orders, and regulations are inconsistent with this order.

SEC. 2. DEFINITIONS. As used in this order:

(a) "Army Field Manual 2-22.3" means FM 2-22.3, Human Intelligence Collector Operations, issued by the Department of the Army on September 6, 2006.

(b) "Army Field Manual 34-52" means FM 34-52, Intelligence Interrogation, issued by the Department of the Army on May 8, 1987.

(c) "Common Article 3" means Article 3 of each of the Geneva Conventions.

(d) "Convention Against Torture" means the Convention Against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment, December 10, 1984, 1465 U.N.T.S. 85, S. Treaty Doc. No. 100 20 (1988).

(e) "Geneva Conventions" means:

- (i) the Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, August 12, 1949 (6 UST 3114);
- (ii) the Convention for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea, August 12, 1949 (6 UST 3217);

(iii) the Convention Relative to the Treatment of Prisoners of War, August 12, 1949 (6 UST 3316); and

(iv) the Convention Relative to the Protection of Civilian Persons in Time of War, August 12, 1949 (6 UST 3516).

(f) “Treated humanely,” “violence to life and person,” “murder of all kinds,” “mutilation,” “cruel treatment,” “torture,” “outrages upon personal dignity,” and “humiliating and degrading treatment” refer to, and have the same meaning as, those same terms in Common Article 3.

(g) The terms “detention facilities” and “detention facility” in section 4(a) of this order do not refer to facilities used only to hold people on a short-term, transitory basis.

SEC. 3. STANDARDS AND PRACTICES FOR INTERROGATION OF INDIVIDUALS IN THE CUSTODY OR CONTROL OF THE UNITED STATES IN ARMED CONFLICTS.

(a) Common Article 3 Standards as a Minimum Baseline. Consistent with the requirements of the Federal torture statute, 18 U.S.C. 2340 2340A, section 1003 of the Detainee Treatment Act of 2005, 42 U.S.C. 2000dd, the Convention Against Torture, Common Article 3, and other laws regulating the treatment and interrogation of individuals detained in any armed conflict, such persons shall in all circumstances be treated humanely and shall not be subjected to violence to life and person (including murder of all kinds, mutilation, cruel treatment, and torture), nor to outrages upon personal dignity (including humiliating and degrading treatment), whenever such individuals are in the custody or under the effective control of an officer, employee, or other agent of the United States Government or detained within a facility owned, operated, or controlled by a department or agency of the United States.

(b) Interrogation Techniques and Interrogation-Related Treatment. Effective immediately, an individual in the custody or under the effective control of an officer, employee, or other agent of the United States Government, or detained within a facility owned, operated, or controlled by a department or agency of the United States, in any armed conflict, shall not be subjected to any interrogation technique or approach, or any treatment related to interrogation, that is not authorized by and listed in Army Field Manual 2-22.3 (Manual). Interrogation techniques, approaches, and treatments described in the Manual shall be implemented strictly in accord with the principles, processes, conditions, and limitations the Manual prescribes. Where processes required by the Manual, such as a requirement of approval by specified Department of Defense officials, are inapposite to a department or an agency other than the Department of Defense, such a department or agency shall use processes that are substantially equivalent to the processes the Manual prescribes for the Department of Defense. Nothing in this section shall preclude the Federal Bureau of Investigation, or other Federal

law enforcement agencies, from continuing to use authorized, non-coercive techniques of interrogation that are designed to elicit voluntary statements and do not involve the use of force, threats, or promises.

(c) Interpretations of Common Article 3 and the Army Field Manual. From this day forward, unless the Attorney General with appropriate consultation provides further guidance, officers, employees, and other agents of the United States Government may, in conducting interrogations, act in reliance upon Army Field Manual 2-22.3, but may not, in conducting interrogations, rely upon any interpretation of the law governing interrogation—including interpretations of Federal criminal laws, the Convention Against Torture, Common Article 3, Army Field Manual 2-22.3, and its predecessor document, Army Field Manual 34-52 – issued by the Department of Justice between September 11, 2001, and January 20, 2009.

SEC. 4. PROHIBITION OF CERTAIN DETENTION FACILITIES, AND RED CROSS ACCESS TO DETAINED INDIVIDUALS.

(a) CIA Detention. The CIA shall close as expeditiously as possible any detention facilities that it currently operates and shall not operate any such detention facility in the future.

(b) International Committee of the Red Cross Access to Detained Individuals. All departments and agencies of the Federal Government shall provide the International Committee of the Red Cross with notification of, and timely access to, any individual detained in any armed conflict in the custody or under the effective control of an officer, employee, or other agent of the United States Government or detained within a facility owned, operated, or controlled by a department or agency of the United States Government, consistent with Department of Defense regulations and policies.

SEC. 5. SPECIAL INTERAGENCY TASK FORCE ON INTERROGATION AND TRANSFER POLICIES.

(a) ESTABLISHMENT OF SPECIAL INTERAGENCY TASK FORCE. There shall be established a Special Task Force on Interrogation and Transfer Policies (Special Task Force) to review interrogation and transfer policies.

(b) MEMBERSHIP. The Special Task Force shall consist of the following members, or their designees:

- (i) the Attorney General, who shall serve as Chair;
- (ii) the Director of National Intelligence, who shall serve as Co-Vice-Chair;
- (iii) the Secretary of Defense, who shall serve as Co-Vice-Chair;
- (iv) the Secretary of State;
- (v) the Secretary of Homeland Security;

- (vi) the Director of the Central Intelligence Agency;
- (vii) the Chairman of the Joint Chiefs of Staff; and
- (viii) other officers or full-time or permanent part time employees of the United States, as determined by the Chair, with the concurrence of the head of the department or agency concerned.

(c) **STAFF.** The Chair may designate officers and employees within the Department of Justice to serve as staff to support the Special Task Force. At the request of the Chair, officers and employees from other departments or agencies may serve on the Special Task Force with the concurrence of the head of the department or agency that employ such individuals. Such staff must be officers or full-time or permanent part-time employees of the United States. The Chair shall designate an officer or employee of the Department of Justice to serve as the Executive Secretary of the Special Task Force.

(d) **OPERATION.** The Chair shall convene meetings of the Special Task Force, determine its agenda, and direct its work. The Chair may establish and direct subgroups of the Special Task Force, consisting exclusively of members of the Special Task Force, to deal with particular subjects.

(e) **MISSION.** The mission of the Special Task Force shall be:

- (i) to study and evaluate whether the interrogation practices and techniques in Army Field Manual 2 22.3, when employed by departments or agencies outside the military, provide an appropriate means of acquiring the intelligence necessary to protect the Nation, and, if warranted, to recommend any additional or different guidance for other departments or agencies; and
- (ii) to study and evaluate the practices of transferring individuals to other nations in order to ensure that such practices comply with the domestic laws, international obligations, and policies of the United States and do not result in the transfer of individuals to other nations to face torture or otherwise for the purpose, or with the effect, of undermining or circumventing the commitments or obligations of the United States to ensure the humane treatment of individuals in its custody or control.

(f) **ADMINISTRATION.** The Special Task Force shall be established for administrative purposes within the Department of Justice and the Department of Justice shall, to the extent permitted by law and subject to the availability of appropriations, provide administrative support and funding for the Special Task Force.

(g) **RECOMMENDATIONS.** The Special Task Force shall provide a report to the President, through the Assistant to the President for National Security Affairs and the Counsel to the President, on the matters set forth in subsection (d) within 180 days of the date of this order, unless the Chair determines that an extension is necessary.

EXECUTIVE ORDER 13491, ENSURING LAWFUL INTERROGATION

(h) TERMINATION. The Chair shall terminate the Special Task Force upon the completion of its duties.

SEC. 6. CONSTRUCTION WITH OTHER LAWS. Nothing in this order shall be construed to affect the obligations of officers, employees, and other agents of the United States Government to comply with all pertinent laws and treaties of the United States governing detention and interrogation, including but not limited to: the Fifth and Eighth Amendments to the United States Constitution; the Federal torture statute, 18 U.S.C. 2340 2340A; the War Crimes Act, 18 U.S.C. 2441; the Federal assault statute, 18 U.S.C. 113; the Federal maiming statute, 18 U.S.C. 114; the Federal “stalking” statute, 18 U.S.C. 2261A; articles 93, 124, 128, and 134 of the Uniform Code of Military Justice, 10 U.S.C. 893, 924, 928, and 934; section 1003 of the Detainee Treatment Act of 2005, 42 U.S.C. 2000dd; section 6(c) of the Military Commissions Act of 2006, Public Law 109 366; the Geneva Conventions; and the Convention Against Torture. Nothing in this order shall be construed to diminish any rights that any individual may have under these or other laws and treaties. This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity against the United States, its departments, agencies, or other entities, its officers or employees, or any other person.

-/S/- Barack Obama
THE WHITE HOUSE,
January 22, 2009

EXECUTIVE ORDER 13526:
CLASSIFIED NATIONAL SECURITY INFORMATION

[Signed: December 29, 2009, Federal Register Vol. 75, No. 2 (January 5, 2010)]

This order prescribes a uniform system for classifying, safeguarding, and declassifying national security information, including information relating to defense against transnational terrorism. Our democratic principles require that the American people be informed of the activities of their Government. Also, our Nation's progress depends on the free flow of information both within the Government and to the American people. Nevertheless, throughout our history, the national defense has required that certain information be maintained in confidence in order to protect our citizens, our democratic institutions, our homeland security, and our interactions with foreign nations. Protecting information critical to our Nation's security and demonstrating our commitment to open Government through accurate and accountable application of classification standards and routine, secure, and effective declassification are equally important priorities.

NOW, THEREFORE, I, BARACK OBAMA, by the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

PART 1—ORIGINAL CLASSIFICATION

SECTION 1.1. CLASSIFICATION STANDARDS.

(a) Information may be originally classified under the terms of this order only if all of the following conditions are met:

- (1) an original classification authority is classifying the information;
- (2) the information is owned by, produced by or for, or is under the control of the United States Government;
- (3) the information falls within one or more of the categories of information listed in section 1.4 of this order; and
- (4) the original classification authority determines that the unauthorized disclosure of the information reasonably could be expected to result in damage to the national security, which includes defense against transnational terrorism, and the original classification authority is able to identify or describe the damage.

(b) If there is significant doubt about the need to classify information, it shall not be classified. This provision does not:

- (1) amplify or modify the substantive criteria or procedures for classification; or
- (2) create any substantive or procedural rights subject to judicial review.
- (c) Classified information shall not be declassified automatically as a result of any unauthorized disclosure of identical or similar information.
- (d) The unauthorized disclosure of foreign government information is presumed to cause damage to the national security.

SEC. 1.2. CLASSIFICATION LEVELS.

- (a) Information may be classified at one of the following three levels:
 - (1) “Top Secret” shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security that the original classification authority is able to identify or describe.
 - (2) “Secret” shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security that the original classification authority is able to identify or describe.
 - (3) “Confidential” shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security that the original classification authority is able to identify or describe.
- (b) Except as otherwise provided by statute, no other terms shall be used to identify United States classified information.
- (c) If there is significant doubt about the appropriate level of classification, it shall be classified at the lower level.

SEC. 1.3. CLASSIFICATION AUTHORITY.

- (a) The authority to classify information originally may be exercised only by:
 - (1) the President and the Vice President;
 - (2) agency heads and officials designated by the President; and
 - (3) United States Government officials delegated this authority pursuant to paragraph (c) of this section.
- (b) Officials authorized to classify information at a specified level are also authorized to classify information at a lower level.
- (c) Delegation of original classification authority.
 - (1) Delegations of original classification authority shall be limited to the minimum required to administer this order. Agency heads are responsible for ensuring that designated subordinate officials have a demonstrable and continuing need to exercise this authority.

(2) "Top Secret" original classification authority may be delegated only by the President, the Vice President, or an agency head or official designated pursuant to paragraph (a)(2) of this section.

(3) "Secret" or "Confidential" original classification authority may be delegated only by the President, the Vice President, an agency head or official designated pursuant to paragraph (a)(2) of this section, or the senior agency official designated under section 5.4(d) of this order, provided that official has been delegated "Top Secret" original classification authority by the agency head.

(4) Each delegation of original classification authority shall be in writing and the authority shall not be redelegated except as provided in this order. Each delegation shall identify the official by name or position.

(5) Delegations of original classification authority shall be reported or made available by name or position to the Director of the Information Security Oversight Office.

(d) All original classification authorities must receive training in proper classification (including the avoidance of over-classification) and declassification as provided in this order and its implementing directives at least once a calendar year. Such training must include instruction on the proper safeguarding of classified information and on the sanctions in section 5.5 of this order that may be brought against an individual who fails to classify information properly or protect classified information from unauthorized disclosure. Original classification authorities who do not receive such mandatory training at least once within a calendar year shall have their classification authority suspended by the agency head or the senior agency official designated under section 5.4(d) of this order until such training has taken place. A waiver may be granted by the agency head, the deputy agency head, or the senior agency official if an individual is unable to receive such training due to unavoidable circumstances. Whenever a waiver is granted, the individual shall receive such training as soon as practicable.

(e) Exceptional cases. When an employee, government contractor, licensee, certificate holder, or grantee of an agency who does not have original classification authority originates information believed by that person to require classification, the information shall be protected in a manner consistent with this order and its implementing directives. The information shall be transmitted promptly as provided under this order or its implementing directives to the agency that has appropriate subject matter interest and classification authority with respect to this information. That agency shall decide within 30 days whether to classify this information.

SEC. 1.4. CLASSIFICATION CATEGORIES.

Information shall not be considered for classification unless its unauthorized disclosure could reasonably be expected to cause identifiable or describable damage to the national security in accordance with section 1.2 of this order, and it pertains to one or more of the following:

- (a) military plans, weapons systems, or operations;
- (b) foreign government information;
- (c) intelligence activities (including covert action), intelligence sources or methods, or cryptology;
- (d) foreign relations or foreign activities of the United States, including confidential sources;
- (e) scientific, technological, or economic matters relating to the national security;
- (f) United States Government programs for safeguarding nuclear materials or facilities;
- (g) vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security; or
- (h) the development, production, or use of weapons of mass destruction.

SEC. 1.5. DURATION OF CLASSIFICATION.

(a) At the time of original classification, the original classification authority shall establish a specific date or event for declassification based on the duration of the national security sensitivity of the information. Upon reaching the date or event, the information shall be automatically declassified. Except for information that should clearly and demonstrably be expected to reveal the identity of a confidential human source or a human intelligence source or key design concepts of weapons of mass destruction, the date or event shall not exceed the time frame established in paragraph (b) of this section.

(b) If the original classification authority cannot determine an earlier specific date or event for declassification, information shall be marked for declassification 10 years from the date of the original decision, unless the original classification authority otherwise determines that the sensitivity of the information requires that it be marked for declassification for up to 25 years from the date of the original decision.

(c) An original classification authority may extend the duration of classification up to 25 years from the date of origin of the document, change the level of classification, or reclassify specific information only when the standards and procedures for classifying information under this order are followed.

(d) No information may remain classified indefinitely. Information marked for an indefinite duration of classification under predecessor orders, for example, marked as "Originating Agency's Determination Required," or classified information that contains incomplete declassification instructions or lacks

declassification instructions shall be declassified in accordance with part 3 of this order.

SEC. 1.6. IDENTIFICATION AND MARKINGS.

(a) At the time of original classification, the following shall be indicated in a manner that is immediately apparent:

(1) one of the three classification levels defined in section 1.2 of this order;

(2) the identity, by name and position, or by personal identifier, of the original classification authority;

(3) the agency and office of origin, if not otherwise evident;

(4) declassification instructions, which shall indicate one of the following:

(A) the date or event for declassification, as prescribed in section 1.5(a);

(B) the date that is 10 years from the date of original classification, as prescribed in section 1.5(b);

(C) the date that is up to 25 years from the date of original classification, as prescribed in section 1.5(b); or

(D) in the case of information that should clearly and demonstrably be expected to reveal the identity of a confidential human source or a human intelligence source or key design concepts of weapons of mass destruction, the marking prescribed in implementing directives issued pursuant to this order; and

(5) a concise reason for classification that, at a minimum, cites the applicable classification categories in section 1.4 of this order.

(b) Specific information required in paragraph (a) of this section may be excluded if it would reveal additional classified information.

(c) With respect to each classified document, the agency originating the document shall, by marking or other means, indicate which portions are classified, with the applicable classification level, and which portions are unclassified. In accordance with standards prescribed in directives issued under this order, the Director of the Information Security Oversight Office may grant and revoke temporary waivers of this requirement. The Director shall revoke any waiver upon a finding of abuse.

(d) Markings or other indicia implementing the provisions of this order, including abbreviations and requirements to safeguard classified working papers, shall conform to the standards prescribed in implementing directives issued pursuant to this order.

- (e) Foreign government information shall retain its original classification markings or shall be assigned a U.S. classification that provides a degree of protection at least equivalent to that required by the entity that furnished the information. Foreign government information retaining its original classification markings need not be assigned a U.S. classification marking provided that the responsible agency determines that the foreign government markings are adequate to meet the purposes served by U.S. classification markings.
- (f) Information assigned a level of classification under this or predecessor orders shall be considered as classified at that level of classification despite the omission of other required markings. Whenever such information is used in the derivative classification process or is reviewed for possible declassification, holders of such information shall coordinate with an appropriate classification authority for the application of omitted markings.
- (g) The classification authority shall, whenever practicable, use a classified addendum whenever classified information constitutes a small portion of an otherwise unclassified document or prepare a product to allow for dissemination at the lowest level of classification possible or in unclassified form.
- (h) Prior to public release, all declassified records shall be appropriately marked to reflect their declassification.

SEC. 1.7. CLASSIFICATION PROHIBITIONS AND LIMITATIONS.

- (a) In no case shall information be classified, continue to be maintained as classified, or fail to be declassified in order to:
 - (1) conceal violations of law, inefficiency, or administrative error;
 - (2) prevent embarrassment to a person, organization, or agency;
 - (3) restrain competition; or
 - (4) prevent or delay the release of information that does not require protection in the interest of the national security.
- (b) Basic scientific research information not clearly related to the national security shall not be classified.
- (c) Information may not be reclassified after declassification and release to the public under proper authority unless:
 - (1) the reclassification is personally approved in writing by the agency head based on a document-by-document determination by the agency that reclassification is required to prevent significant and demonstrable damage to the national security;
 - (2) the information may be reasonably recovered without bringing undue attention to the information;
 - (3) the reclassification action is reported promptly to the Assistant to the President for National Security Affairs (National Security Advisor) and the Director of the Information Security Oversight Office; and

(4) for documents in the physical and legal custody of the National Archives and Records Administration (National Archives) that have been available for public use, the agency head has, after making the determinations required by this paragraph, notified the Archivist of the United States (Archivist), who shall suspend public access pending approval of the reclassification action by the Director of the Information Security Oversight Office. Any such decision by the Director may be appealed by the agency head to the President through the National Security Advisor. Public access shall remain suspended pending a prompt decision on the appeal.

(d) Information that has not previously been disclosed to the public under proper authority may be classified or reclassified after an agency has received a request for it under the Freedom of Information Act (5 U.S.C. 552), the Presidential Records Act, 44 U.S.C. 2204(c)(1), the Privacy Act of 1974 (5 U.S.C. 552a), or the mandatory review provisions of section 3.5 of this order only if such classification meets the requirements of this order and is accomplished on a document-by-document basis with the personal participation or under the direction of the agency head, the deputy agency head, or the senior agency official designated under section 5.4 of this order. The requirements in this paragraph also apply to those situations in which information has been declassified in accordance with a specific date or event determined by an original classification authority in accordance with section 1.5 of this order.

(e) Compilations of items of information that are individually unclassified may be classified if the compiled information reveals an additional association or relationship that:

- (1) meets the standards for classification under this order; and
- (2) is not otherwise revealed in the individual items of information.

SEC. 1.8. CLASSIFICATION CHALLENGES.

(a) Authorized holders of information who, in good faith, believe that its classification status is improper are encouraged and expected to challenge the classification status of the information in accordance with agency procedures established under paragraph (b) of this section.

(b) In accordance with implementing directives issued pursuant to this order, an agency head or senior agency official shall establish procedures under which authorized holders of information, including authorized holders outside the classifying agency, are encouraged and expected to challenge the classification of information that they believe is improperly classified or unclassified. These procedures shall ensure that:

- (1) individuals are not subject to retribution for bringing such actions;

(2) an opportunity is provided for review by an impartial official or panel; and

(3) individuals are advised of their right to appeal agency decisions to the Interagency Security Classification Appeals Panel (Panel) established by section 5.3 of this order.

(c) Documents required to be submitted for prepublication review or other administrative process pursuant to an approved nondisclosure agreement are not covered by this section.

SEC. 1.9. FUNDAMENTAL CLASSIFICATION GUIDANCE REVIEW.

(a) Agency heads shall complete on a periodic basis a comprehensive review of the agency's classification guidance, particularly classification guides, to ensure the guidance reflects current circumstances and to identify classified information that no longer requires protection and can be declassified. The initial fundamental classification guidance review shall be completed within 2 years of the effective date of this order.

(b) The classification guidance review shall include an evaluation of classified information to determine if it meets the standards for classification under section 1.4 of this order, taking into account an up-to-date assessment of likely damage as described under section 1.2 of this order.

(c) The classification guidance review shall include original classification authorities and agency subject matter experts to ensure a broad range of perspectives.

(d) Agency heads shall provide a report summarizing the results of the classification guidance review to the Director of the Information Security Oversight Office and shall release an unclassified version of this report to the public.

PART 2—DERIVATIVE CLASSIFICATION

SEC. 2.1. USE OF DERIVATIVE CLASSIFICATION.

(a) Persons who reproduce, extract, or summarize classified information, or who apply classification markings derived from source material or as directed by a classification guide, need not possess original classification authority.

(b) Persons who apply derivative classification markings shall:

(1) be identified by name and position, or by personal identifier, in a manner that is immediately apparent for each derivative classification action;

(2) observe and respect original classification decisions; and

(3) carry forward to any newly created documents the pertinent classification markings. For information derivatively classified based on multiple sources, the derivative classifier shall carry forward:

(A) the date or event for declassification that corresponds to the longest period of classification among the sources, or the marking established pursuant to section 1.6(a)(4)(D) of this order; and

(B) a listing of the source materials.

(c) Derivative classifiers shall, whenever practicable, use a classified addendum whenever classified information constitutes a small portion of an otherwise unclassified document or prepare a product to allow for dissemination at the lowest level of classification possible or in unclassified form.

(d) Persons who apply derivative classification markings shall receive training in the proper application of the derivative classification principles of the order, with an emphasis on avoiding over-classification, at least once every 2 years.

Derivative classifiers who do not receive such training at least once every 2 years shall have their authority to apply derivative classification markings suspended until they have received such training. A waiver may be granted by the agency head, the deputy agency head, or the senior agency official if an individual is unable to receive such training due to unavoidable circumstances. Whenever a waiver is granted, the individual shall receive such training as soon as practicable.

SEC. 2.2. CLASSIFICATION GUIDES.

(a) Agencies with original classification authority shall prepare classification guides to facilitate the proper and uniform derivative classification of information. These guides shall conform to standards contained in directives issued under this order.

(b) Each guide shall be approved personally and in writing by an official who:

(1) has program or supervisory responsibility over the information or is the senior agency official; and

(2) is authorized to classify information originally at the highest level of classification prescribed in the guide.

(c) Agencies shall establish procedures to ensure that classification guides are reviewed and updated as provided in directives issued under this order.

(d) Agencies shall incorporate original classification decisions into classification guides on a timely basis and in accordance with directives issued under this order.

(e) Agencies may incorporate exemptions from automatic declassification approved pursuant to section 3.3(j) of this order into classification guides,

provided that the Panel is notified of the intent to take such action for specific information in advance of approval and the information remains in active use.

(f) The duration of classification of a document classified by a derivative classifier using a classification guide shall not exceed 25 years from the date of the origin of the document, except for:

- (1) information that should clearly and demonstrably be expected to reveal the identity of a confidential human source or a human intelligence source or key design concepts of weapons of mass destruction; and
- (2) specific information incorporated into classification guides in accordance with section 2.2(e) of this order.

PART 3—DECLASSIFICATION AND DOWNGRADING

SEC. 3.1. AUTHORITY FOR DECLASSIFICATION.

(a) Information shall be declassified as soon as it no longer meets the standards for classification under this order.

(b) Information shall be declassified or downgraded by:

- (1) the official who authorized the original classification, if that official is still serving in the same position and has original classification authority;
- (2) the originator's current successor in function, if that individual has original classification authority;
- (3) a supervisory official of either the originator or his or her successor in function, if the supervisory official has original classification authority; or
- (4) officials delegated declassification authority in writing by the agency head or the senior agency official of the originating agency.

(c) The Director of National Intelligence (or, if delegated by the Director of National Intelligence, the Principal Deputy Director of National Intelligence) may, with respect to the Intelligence Community, after consultation with the head of the originating Intelligence Community element or department, declassify, downgrade, or direct the declassification or downgrading of information or intelligence relating to intelligence sources, methods, or activities.

(d) It is presumed that information that continues to meet the classification requirements under this order requires continued protection. In some exceptional cases, however, the need to protect such information may be outweighed by the public interest in disclosure of the information, and in these cases the information should be declassified. When such questions arise, they shall be referred to the agency head or the senior agency official. That official will determine, as an exercise of discretion, whether the public interest in disclosure outweighs the

damage to the national security that might reasonably be expected from disclosure. This provision does not:

(1) amplify or modify the substantive criteria or procedures for classification; or

(2) create any substantive or procedural rights subject to judicial review.

(e) If the Director of the Information Security Oversight Office determines that information is classified in violation of this order, the Director may require the information to be declassified by the agency that originated the classification. Any such decision by the Director may be appealed to the President through the National Security Advisor. The information shall remain classified pending a prompt decision on the appeal.

(f) The provisions of this section shall also apply to agencies that, under the terms of this order, do not have original classification authority, but had such authority under predecessor orders.

(g) No information may be excluded from declassification under section 3.3 of this order based solely on the type of document or record in which it is found. Rather, the classified information must be considered on the basis of its content.

(h) Classified nonrecord materials, including artifacts, shall be declassified as soon as they no longer meet the standards for classification under this order.

(i) When making decisions under sections 3.3, 3.4, and 3.5 of this order, agencies shall consider the final decisions of the Panel.

SEC. 3.2. TRANSFERRED RECORDS.

(a) In the case of classified records transferred in conjunction with a transfer of functions, and not merely for storage purposes, the receiving agency shall be deemed to be the originating agency for purposes of this order.

(b) In the case of classified records that are not officially transferred as described in paragraph (a) of this section, but that originated in an agency that has ceased to exist and for which there is no successor agency, each agency in possession of such records shall be deemed to be the originating agency for purposes of this order. Such records may be declassified or downgraded by the agency in possession of the records after consultation with any other agency that has an interest in the subject matter of the records.

(c) Classified records accessioned into the National Archives shall be declassified or downgraded by the Archivist in accordance with this order, the directives issued pursuant to this order, agency declassification guides, and any existing procedural agreement between the Archivist and the relevant agency head.

(d) The originating agency shall take all reasonable steps to declassify classified information contained in records determined to have permanent historical value before they are accessioned into the National Archives. However, the Archivist may require that classified records be accessioned into the National Archives

when necessary to comply with the provisions of the Federal Records Act. This provision does not apply to records transferred to the Archivist pursuant to section 2203 of title 44, United States Code, or records for which the National Archives serves as the custodian of the records of an agency or organization that has gone out of existence.

(e) To the extent practicable, agencies shall adopt a system of records management that will facilitate the public release of documents at the time such documents are declassified pursuant to the provisions for automatic declassification in section 3.3 of this order.

SEC. 3.3. AUTOMATIC DECLASSIFICATION.

(a) Subject to paragraphs (b)–(d) and (g)–(j) of this section, all classified records that (1) are more than 25 years old and (2) have been determined to have permanent historical value under title 44, United States Code, shall be automatically declassified whether or not the records have been reviewed. All classified records shall be automatically declassified on December 31 of the year that is 25 years from the date of origin, except as provided in paragraphs (b)–(d) and (g)–(j) of this section. If the date of origin of an individual record cannot be readily determined, the date of original classification shall be used instead.

(b) An agency head may exempt from automatic declassification under paragraph (a) of this section specific information, the release of which should clearly and demonstrably be expected to:

- (1) reveal the identity of a confidential human source, a human intelligence source, a relationship with an intelligence or security service of a foreign government or international organization, or a nonhuman intelligence source; or impair the effectiveness of an intelligence method currently in use, available for use, or under development;
- (2) reveal information that would assist in the development, production, or use of weapons of mass destruction;
- (3) reveal information that would impair U.S. cryptologic systems or activities;
- (4) reveal information that would impair the application of state-of-the-art technology within a U.S. weapon system;
- (5) reveal formally named or numbered U.S. military war plans that remain in effect, or reveal operational or tactical elements of prior plans that are contained in such active plans;
- (6) reveal information, including foreign government information, that would cause serious harm to relations between the United States and a foreign government, or to ongoing diplomatic activities of the United States;

(7) reveal information that would impair the current ability of United States Government officials to protect the President, Vice President, and other protectees for whom protection services, in the interest of the national security, are authorized;

(8) reveal information that would seriously impair current national security emergency preparedness plans or reveal current vulnerabilities of systems, installations, or infrastructures relating to the national security; or

(9) violate a statute, treaty, or international agreement that does not permit the automatic or unilateral declassification of information at 25 years.

(c)(1) An agency head shall notify the Panel of any specific file series of records for which a review or assessment has determined that the information within that file series almost invariably falls within one or more of the exemption categories listed in paragraph (b) of this section and that the agency proposes to exempt from automatic declassification at 25 years.

(2) The notification shall include:

(A) a description of the file series;

(B) an explanation of why the information within the file series is almost invariably exempt from automatic declassification and why the information must remain classified for a longer period of time; and

(C) except when the information within the file series almost invariably identifies a confidential human source or a human intelligence source or key design concepts of weapons of mass destruction, a specific date or event for declassification of the information, not to exceed December 31 of the year that is 50 years from the date of origin of the records.

(3) The Panel may direct the agency not to exempt a designated file series or to declassify the information within that series at an earlier date than recommended. The agency head may appeal such a decision to the President through the National Security Advisor.

(4) File series exemptions approved by the President prior to December 31, 2008, shall remain valid without any additional agency action pending Panel review by the later of December 31, 2010, or December 31 of the year that is 10 years from the date of previous approval.

(d) The following provisions shall apply to the onset of automatic declassification:

(1) Classified records within an integral file block, as defined in this order, that are otherwise subject to automatic declassification under this section shall not be automatically declassified until December 31 of the

year that is 25 years from the date of the most recent record within the file block.

(2) After consultation with the Director of the National Declassification Center (the Center) established by section 3.7 of this order and before the records are subject to automatic declassification, an agency head or senior agency official may delay automatic declassification for up to five additional years for classified information contained in media that make a review for possible declassification exemptions more difficult or costly.

(3) Other than for records that are properly exempted from automatic declassification, records containing classified information that originated with other agencies or the disclosure of which would affect the interests or activities of other agencies with respect to the classified information and could reasonably be expected to fall under one or more of the exemptions in paragraph (b) of this section shall be identified prior to the onset of automatic declassification for later referral to those agencies.

(A) The information of concern shall be referred by the Center established by section 3.7 of this order, or by the centralized facilities referred to in section 3.7(e) of this order, in a prioritized and scheduled manner determined by the Center.

(B) If an agency fails to provide a final determination on a referral made by the Center within 1 year of referral, or by the centralized facilities referred to in section 3.7(e) of this order within 3 years of referral, its equities in the referred records shall be automatically declassified.

(C) If any disagreement arises between affected agencies and the Center regarding the referral review period, the Director of the Information Security Oversight Office shall determine the appropriate period of review of referred records.

(D) Referrals identified prior to the establishment of the Center by section 3.7 of this order shall be subject to automatic declassification only in accordance with subparagraphs (d)(3)(A)–(C) of this section.

(4) After consultation with the Director of the Information Security Oversight Office, an agency head may delay automatic declassification for up to 3 years from the date of discovery of classified records that were inadvertently not reviewed prior to the effective date of automatic declassification.

(e) Information exempted from automatic declassification under this section shall remain subject to the mandatory and systematic declassification review provisions of this order.

(f) The Secretary of State shall determine when the United States should commence negotiations with the appropriate officials of a foreign government or international organization of governments to modify any treaty or international agreement that requires the classification of information contained in records affected by this section for a period longer than 25 years from the date of its creation, unless the treaty or international agreement pertains to information that may otherwise remain classified beyond 25 years under this section.

(g) The Secretary of Energy shall determine when information concerning foreign nuclear programs that was removed from the Restricted Data category in order to carry out provisions of the National Security Act of 1947, as amended, may be declassified. Unless otherwise determined, such information shall be declassified when comparable information concerning the United States nuclear program is declassified.

(h) Not later than 3 years from the effective date of this order, all records exempted from automatic declassification under paragraphs (b) and (c) of this section shall be automatically declassified on December 31 of a year that is no more than 50 years from the date of origin, subject to the following:

(1) Records that contain information the release of which should clearly and demonstrably be expected to reveal the following are exempt from automatic declassification at 50 years:

(A) the identity of a confidential human source or a human intelligence source; or

(B) key design concepts of weapons of mass destruction.

(2) In extraordinary cases, agency heads may, within 5 years of the onset of automatic declassification, propose to exempt additional specific information from declassification at 50 years.

(3) Records exempted from automatic declassification under this paragraph shall be automatically declassified on December 31 of a year that is no more than 75 years from the date of origin unless an agency head, within 5 years of that date, proposes to exempt specific information from declassification at 75 years and the proposal is formally approved by the Panel.

(i) Specific records exempted from automatic declassification prior to the establishment of the Center described in section 3.7 of this order shall be subject to the provisions of paragraph (h) of this section in a scheduled and prioritized manner determined by the Center.

(j) At least 1 year before information is subject to automatic declassification under this section, an agency head or senior agency official shall notify the Director of the Information Security Oversight Office, serving as Executive Secretary of the Panel, of any specific information that the agency proposes to

exempt from automatic declassification under paragraphs (b) and (h) of this section.

(1) The notification shall include:

(A) a detailed description of the information, either by reference to information in specific records or in the form of a declassification guide;

(B) an explanation of why the information should be exempt from automatic declassification and must remain classified for a longer period of time; and

(C) a specific date or a specific and independently verifiable event for automatic declassification of specific records that contain the information proposed for exemption.

(2) The Panel may direct the agency not to exempt the information or to declassify it at an earlier date than recommended. An agency head may appeal such a decision to the President through the National Security Advisor. The information will remain classified while such an appeal is pending.

(k) For information in a file series of records determined not to have permanent historical value, the duration of classification beyond 25 years shall be the same as the disposition (destruction) date of those records in each Agency Records Control Schedule or General Records Schedule, although the duration of classification shall be extended if the record has been retained for business reasons beyond the scheduled disposition date.

SEC. 3.4. SYSTEMATIC DECLASSIFICATION REVIEW.

(a) Each agency that has originated classified information under this order or its predecessors shall establish and conduct a program for systematic declassification review for records of permanent historical value exempted from automatic declassification under section 3.3 of this order. Agencies shall prioritize their review of such records in accordance with priorities established by the Center.

(b) The Archivist shall conduct a systematic declassification review program for classified records:

(1) accessioned into the National Archives;

(2) transferred to the Archivist pursuant to 44 U.S.C. 2203; and

(3) for which the National Archives serves as the custodian for an agency or organization that has gone out of existence.

SEC. 3.5. MANDATORY DECLASSIFICATION REVIEW.

(a) Except as provided in paragraph (b) of this section, all information classified under this order or predecessor orders shall be subject to a review for declassification by the originating agency if:

- (1) the request for a review describes the document or material containing the information with sufficient specificity to enable the agency to locate it with a reasonable amount of effort;
- (2) the document or material containing the information responsive to the request is not contained within an operational file exempted from search and review, publication, and disclosure under 5 U.S.C. 552 in accordance with law; and
- (3) the information is not the subject of pending litigation.

(b) Information originated by the incumbent President or the incumbent Vice President; the incumbent President's White House Staff or the incumbent Vice President's Staff; committees, commissions, or boards appointed by the incumbent President; or other entities within the Executive Office of the President that solely advise and assist the incumbent President is exempted from the provisions of paragraph (a) of this section. However, the Archivist shall have the authority to review, downgrade, and declassify papers or records of former Presidents and Vice Presidents under the control of the Archivist pursuant to 44 U.S.C. 2107, 2111, 2111 note, or 2203. Review procedures developed by the Archivist shall provide for consultation with agencies having primary subject matter interest and shall be consistent with the provisions of applicable laws or lawful agreements that pertain to the respective Presidential papers or records. Agencies with primary subject matter interest shall be notified promptly of the archivist's decision. Any final decision by the Archivist may be appealed by the requester or an agency to the Panel. The information shall remain classified pending a prompt decision on the appeal.

(c) Agencies conducting a mandatory review for declassification shall declassify information that no longer meets the standards for classification under this order. They shall release this information unless withholding is otherwise authorized and warranted under applicable law.

(d) If an agency has reviewed the requested information for declassification within the past 2 years, the agency need not conduct another review and may instead inform the requester of this fact and the prior review decision and advise the requester of appeal rights provided under subsection (e) of this section.

(e) In accordance with directives issued pursuant to this order, agency heads shall develop procedures to process requests for the mandatory review of classified information. These procedures shall apply to information classified under this or predecessor orders. They also shall provide a means for administratively

appealing a denial of a mandatory review request, and for notifying the requester of the right to appeal a final agency decision to the Panel.

(f) After consultation with affected agencies, the Secretary of Defense shall develop special procedures for the review of cryptologic information; the Director of National Intelligence shall develop special procedures for the review of information pertaining to intelligence sources, methods, and activities; and the Archivist shall develop special procedures for the review of information accessioned into the National Archives.

(g) Documents required to be submitted for prepublication review or other administrative process pursuant to an approved nondisclosure agreement are not covered by this section.

(h) This section shall not apply to any request for a review made to an element of the Intelligence Community that is made by a person other than an individual as that term is defined by 5 U.S.C. 552a(a)(2), or by a foreign government entity or any representative thereof.

SEC. 3.6. PROCESSING REQUESTS AND REVIEWS.

Notwithstanding section 4.1(i) of this order, in response to a request for information under the Freedom of Information Act, the Presidential Records Act, the Privacy Act of 1974, or the mandatory review provisions of this order:

(a) An agency may refuse to confirm or deny the existence or nonexistence of requested records whenever the fact of their existence or nonexistence is itself classified under this order or its predecessors.

(b) When an agency receives any request for documents in its custody that contain classified information that originated with other agencies or the disclosure of which would affect the interests or activities of other agencies with respect to the classified information, or identifies such documents in the process of implementing sections 3.3 or 3.4 of this order, it shall refer copies of any request and the pertinent documents to the originating agency for processing and may, after consultation with the originating agency, inform any requester of the referral unless such association is itself classified under this order or its predecessors. In cases in which the originating agency determines in writing that a response under paragraph (a) of this section is required, the referring agency shall respond to the requester in accordance with that paragraph.

(c) Agencies may extend the classification of information in records determined not to have permanent historical value or nonrecord materials, including artifacts, beyond the time frames established in sections 1.5(b) and 2.2(f) of this order, provided:

- (1) the specific information has been approved pursuant to section 3.3(j) of this order for exemption from automatic declassification; and

(2) the extension does not exceed the date established in section 3.3(j) of this order.

SEC. 3.7. NATIONAL DECLASSIFICATION CENTER.

(a) There is established within the National Archives a National Declassification Center to streamline declassification processes, facilitate quality-assurance measures, and implement standardized training regarding the declassification of records determined to have permanent historical value. There shall be a Director of the Center who shall be appointed or removed by the Archivist in consultation with the Secretaries of State, Defense, Energy, and Homeland Security, the Attorney General, and the Director of National Intelligence.

(b) Under the administration of the Director, the Center shall coordinate:

(1) timely and appropriate processing of referrals in accordance with section 3.3(d)(3) of this order for accessioned Federal records and transferred presidential records.

(2) general interagency declassification activities necessary to fulfill the requirements of sections 3.3 and 3.4 of this order;

(3) the exchange among agencies of detailed declassification guidance to enable the referral of records in accordance with section 3.3(d)(3) of this order;

(4) the development of effective, transparent, and standard declassification work processes, training, and quality assurance measures;

(5) the development of solutions to declassification challenges posed by electronic records, special media, and emerging technologies;

(6) the linkage and effective utilization of existing agency databases and the use of new technologies to document and make public declassification review decisions and support declassification activities under the purview of the Center; and

(7) storage and related services, on a reimbursable basis, for Federal records containing classified national security information.

(c) Agency heads shall fully cooperate with the Archivist in the activities of the Center and shall:

(1) provide the Director with adequate and current declassification guidance to enable the referral of records in accordance with section 3.3(d)(3) of this order; and

(2) upon request of the Archivist, assign agency personnel to the Center who shall be delegated authority by the agency head to review and exempt or declassify information originated by their agency contained in records accessioned into the National Archives, after consultation with subject matter experts as necessary.

- (d) The Archivist, in consultation with representatives of the participants in the Center and after input from the general public, shall develop priorities for declassification activities under the purview of the Center that take into account the degree of researcher interest and the likelihood of declassification.
- (e) Agency heads may establish such centralized facilities and internal operations to conduct internal declassification reviews as appropriate to achieve optimized records management and declassification business processes. Once established, all referral processing of accessioned records shall take place at the Center, and such agency facilities and operations shall be coordinated with the Center to ensure the maximum degree of consistency in policies and procedures that relate to records determined to have permanent historical value.
- (f) Agency heads may exempt from automatic declassification or continue the classification of their own originally classified information under section 3.3(a) of this order except that in the case of the Director of National Intelligence, the Director shall also retain such authority with respect to the Intelligence Community.
- (g) The Archivist shall, in consultation with the Secretaries of State, Defense, Energy, and Homeland Security, the Attorney General, the Director of National Intelligence, the Director of the Central Intelligence Agency, and the Director of the Information Security Oversight Office, provide the National Security Advisor with a detailed concept of operations for the Center and a proposed implementing directive under section 5.1 of this order that reflects the coordinated views of the aforementioned agencies.

PART 4—SAFEGUARDING

SEC. 4.1. GENERAL RESTRICTIONS ON ACCESS.

- (a) A person may have access to classified information provided that:
- (1) a favorable determination of eligibility for access has been made by an agency head or the agency head's designee;
 - (2) the person has signed an approved nondisclosure agreement; and
 - (3) the person has a need-to-know the information.
- (b) Every person who has met the standards for access to classified information in paragraph (a) of this section shall receive contemporaneous training on the proper safeguarding of classified information and on the criminal, civil, and administrative sanctions that may be imposed on an individual who fails to protect classified information from unauthorized disclosure.
- (c) An official or employee leaving agency service may not remove classified information from the agency's control or direct that information be declassified in order to remove it from agency control.

- (d) Classified information may not be removed from official premises without proper authorization.
- (e) Persons authorized to disseminate classified information outside the executive branch shall ensure the protection of the information in a manner equivalent to that provided within the executive branch.
- (f) Consistent with law, executive orders, directives, and regulations, an agency head or senior agency official or, with respect to the Intelligence Community, the Director of National Intelligence, shall establish uniform procedures to ensure that automated information systems, including networks and telecommunications systems, that collect, create, communicate, compute, disseminate, process, or store classified information:
- (1) prevent access by unauthorized persons;
 - (2) ensure the integrity of the information; and
 - (3) to the maximum extent practicable, use:
 - (A) common information technology standards, protocols, and interfaces that maximize the availability of, and access to, the information in a form and manner that facilitates its authorized use; and
 - (B) standardized electronic formats to maximize the accessibility of information to persons who meet the criteria set forth in section 4.1(a) of this order.
- (g) Consistent with law, executive orders, directives, and regulations, each agency head or senior agency official, or with respect to the Intelligence Community, the Director of National Intelligence, shall establish controls to ensure that classified information is used, processed, stored, reproduced, transmitted, and destroyed under conditions that provide adequate protection and prevent access by unauthorized persons.
- (h) Consistent with directives issued pursuant to this order, an agency shall safeguard foreign government information under standards that provide a degree of protection at least equivalent to that required by the government or international organization of governments that furnished the information. When adequate to achieve equivalency, these standards may be less restrictive than the safeguarding standards that ordinarily apply to U.S. “Confidential” information, including modified handling and transmission and allowing access to individuals with a need-to-know who have not otherwise been cleared for access to classified information or executed an approved nondisclosure agreement.
- (i)(1) Classified information originating in one agency may be disseminated to another agency or U.S. entity by any agency to which it has been made available without the consent of the originating agency, as long as the criteria for access under section 4.1(a) of this order are met, unless the originating agency has determined that prior authorization is required for such dissemination and has

marked or indicated such requirement on the medium containing the classified information in accordance with implementing directives issued pursuant to this order.

(2) Classified information originating in one agency may be disseminated by any other agency to which it has been made available to a foreign government in accordance with statute, this order, directives implementing this order, direction of the President, or with the consent of the originating agency. For the purposes of this section, “foreign government” includes any element of a foreign government, or an international organization of governments, or any element thereof.

(3) Documents created prior to the effective date of this order shall not be disseminated outside any other agency to which they have been made available without the consent of the originating agency. An agency head or senior agency official may waive this requirement for specific information that originated within that agency.

(4) For purposes of this section, the Department of Defense shall be considered one agency, except that any dissemination of information regarding intelligence sources, methods, or activities shall be consistent with directives issued pursuant to section 6.2(b) of this order.

(5) Prior consent of the originating agency is not required when referring records for declassification review that contain information originating in more than one agency.

SEC. 4.2. DISTRIBUTION CONTROLS.

(a) The head of each agency shall establish procedures in accordance with applicable law and consistent with directives issued pursuant to this order to ensure that classified information is accessible to the maximum extent possible by individuals who meet the criteria set forth in section 4.1(a) of this order.

(b) In an emergency, when necessary to respond to an imminent threat to life or in defense of the homeland, the agency head or any designee may authorize the disclosure of classified information (including information marked pursuant to section 4.1(i)(1) of this order) to an individual or individuals who are otherwise not eligible for access. Such actions shall be taken only in accordance with directives implementing this order and any procedure issued by agencies governing the classified information, which shall be designed to minimize the classified information that is disclosed under these circumstances and the number of individuals who receive it. Information disclosed under this provision or implementing directives and procedures shall not be deemed declassified as a result of such disclosure or subsequent use by a recipient. Such disclosures shall be reported promptly to the originator of the classified information. For purposes of this section, the Director of National Intelligence may issue an implementing

directive governing the emergency disclosure of classified intelligence information.

(c) Each agency shall update, at least annually, the automatic, routine, or recurring distribution mechanism for classified information that it distributes. Recipients shall cooperate fully with distributors who are updating distribution lists and shall notify distributors whenever a relevant change in status occurs.

SEC. 4.3. SPECIAL ACCESS PROGRAMS.

(a) ESTABLISHMENT OF SPECIAL ACCESS PROGRAMS. Unless otherwise authorized by the President, only the Secretaries of State, Defense, Energy, and Homeland Security, the Attorney General, and the Director of National Intelligence, or the principal deputy of each, may create a special access program. For special access programs pertaining to intelligence sources, methods, and activities (but not including military operational, strategic, and tactical programs), this function shall be exercised by the Director of National Intelligence. These officials shall keep the number of these programs at an absolute minimum, and shall establish them only when the program is required by statute or upon a specific finding that:

- (1) the vulnerability of, or threat to, specific information is exceptional; and
- (2) the normal criteria for determining eligibility for access applicable to information classified at the same level are not deemed sufficient to protect the information from unauthorized disclosure.

(b) REQUIREMENTS AND LIMITATIONS.

- (1) Special access programs shall be limited to programs in which the number of persons who ordinarily will have access will be reasonably small and commensurate with the objective of providing enhanced protection for the information involved.
- (2) Each agency head shall establish and maintain a system of accounting for special access programs consistent with directives issued pursuant to this order.
- (3) Special access programs shall be subject to the oversight program established under section 5.4(d) of this order. In addition, the Director of the Information Security Oversight Office shall be afforded access to these programs, in accordance with the security requirements of each program, in order to perform the functions assigned to the Information Security Oversight Office under this order. An agency head may limit access to a special access program to the Director of the Information Security Oversight Office and no more than one other employee of the Information Security Oversight Office or, for special access programs that are extraordinarily sensitive and vulnerable, to the Director only.

(4) The agency head or principal deputy shall review annually each special access program to determine whether it continues to meet the requirements of this order.

(5) Upon request, an agency head shall brief the National Security Advisor, or a designee, on any or all of the agency's special access programs.

(6) For the purposes of this section, the term "agency head" refers only to the Secretaries of State, Defense, Energy, and Homeland Security, the Attorney General, and the Director of National Intelligence, or the principal deputy of each.

(c) Nothing in this order shall supersede any requirement made by or under 10 U.S.C. 119.

SEC. 4.4. ACCESS BY HISTORICAL RESEARCHERS AND CERTAIN FORMER GOVERNMENT PERSONNEL.

(a) The requirement in section 4.1(a)(3) of this order that access to classified information may be granted only to individuals who have a need-to-know the information may be waived for persons who:

(1) are engaged in historical research projects;

(2) previously have occupied senior policy-making positions to which they were appointed or designated by the President or the Vice President; or

(3) served as President or Vice President.

(b) Waivers under this section may be granted only if the agency head or senior agency official of the originating agency:

(1) determines in writing that access is consistent with the interest of the national security;

(2) takes appropriate steps to protect classified information from unauthorized disclosure or compromise, and ensures that the information is safeguarded in a manner consistent with this order; and

(3) limits the access granted to former Presidential appointees or designees and Vice Presidential appointees or designees to items that the person originated, reviewed, signed, or received while serving as a Presidential or Vice Presidential appointee or designee.

PART 5—IMPLEMENTATION AND REVIEW

SEC. 5.1. PROGRAM DIRECTION.

(a) The Director of the Information Security Oversight Office, under the direction of the Archivist and in consultation with the National Security Advisor, shall issue such directives as are necessary to implement this order. These directives

shall be binding on the agencies. Directives issued by the Director of the Information Security Oversight Office shall establish standards for:

- (1) classification, declassification, and marking principles;
- (2) safeguarding classified information, which shall pertain to the handling, storage, distribution, transmittal, and destruction of and accounting for classified information;
- (3) agency security education and training programs;
- (4) agency self-inspection programs; and
- (5) classification and declassification guides.

(b) The Archivist shall delegate the implementation and monitoring functions of this program to the Director of the Information Security Oversight Office.

(c) The Director of National Intelligence, after consultation with the heads of affected agencies and the Director of the Information Security Oversight Office, may issue directives to implement this order with respect to the protection of intelligence sources, methods, and activities. Such directives shall be consistent with this order and directives issued under paragraph (a) of this section.

SEC. 5.2. INFORMATION SECURITY OVERSIGHT OFFICE.

(a) There is established within the National Archives an Information Security Oversight Office. The Archivist shall appoint the Director of the Information Security Oversight Office, subject to the approval of the President.

(b) Under the direction of the Archivist, acting in consultation with the National Security Advisor, the Director of the Information Security Oversight Office shall:

- (1) develop directives for the implementation of this order;
- (2) oversee agency actions to ensure compliance with this order and its implementing directives;
- (3) review and approve agency implementing regulations prior to their issuance to ensure their consistency with this order and directives issued under section 5.1(a) of this order;
- (4) have the authority to conduct on-site reviews of each agency's program established under this order, and to require of each agency those reports and information and other cooperation that may be necessary to fulfill its responsibilities. If granting access to specific categories of classified information would pose an exceptional national security risk, the affected agency head or the senior agency official shall submit a written justification recommending the denial of access to the President through the National Security Advisor within 60 days of the request for access. Access shall be denied pending the response;
- (5) review requests for original classification authority from agencies or officials not granted original classification authority and, if deemed

appropriate, recommend Presidential approval through the National Security Advisor;

(6) consider and take action on complaints and suggestions from persons within or outside the Government with respect to the administration of the program established under this order;

(7) have the authority to prescribe, after consultation with affected agencies, standardization of forms or procedures that will promote the implementation of the program established under this order;

(8) report at least annually to the President on the implementation of this order; and

(9) convene and chair interagency meetings to discuss matters pertaining to the program established by this order.

SEC. 5.3. INTERAGENCY SECURITY CLASSIFICATION APPEALS PANEL.

(a) ESTABLISHMENT AND ADMINISTRATION.

(1) There is established an Interagency Security Classification Appeals Panel. The Departments of State, Defense, and Justice, the National Archives, the Office of the Director of National Intelligence, and the National Security Advisor shall each be represented by a senior-level representative who is a full-time or permanent part-time Federal officer or employee designated to serve as a member of the Panel by the respective agency head. The President shall designate a Chair from among the members of the Panel.

(2) Additionally, the Director of the Central Intelligence Agency may appoint a temporary representative who meets the criteria in paragraph (a)(1) of this section to participate as a voting member in all Panel deliberations and associated support activities concerning classified information originated by the Central Intelligence Agency.

(3) A vacancy on the Panel shall be filled as quickly as possible as provided in paragraph (a)(1) of this section.

(4) The Director of the Information Security Oversight Office shall serve as the Executive Secretary of the Panel. The staff of the Information Security Oversight Office shall provide program and administrative support for the Panel.

(5) The members and staff of the Panel shall be required to meet eligibility for access standards in order to fulfill the Panel's functions.

(6) The Panel shall meet at the call of the Chair. The Chair shall schedule meetings as may be necessary for the Panel to fulfill its functions in a timely manner.

(7) The Information Security Oversight Office shall include in its reports to the President a summary of the Panel's activities.

(b) FUNCTIONS. The Panel shall:

- (1) decide on appeals by persons who have filed classification challenges under section 1.8 of this order;
- (2) approve, deny, or amend agency exemptions from automatic declassification as provided in section 3.3 of this order;
- (3) decide on appeals by persons or entities who have filed requests for mandatory declassification review under section 3.5 of this order; and
- (4) appropriately inform senior agency officials and the public of final Panel decisions on appeals under sections 1.8 and 3.5 of this order.

(c) RULES AND PROCEDURES. The Panel shall issue bylaws, which shall be published in the *Federal Register*. The bylaws shall establish the rules and procedures that the Panel will follow in accepting, considering, and issuing decisions on appeals. The rules and procedures of the Panel shall provide that the Panel will consider appeals only on actions in which:

- (1) the appellant has exhausted his or her administrative remedies within the responsible agency;
- (2) there is no current action pending on the issue within the Federal courts; and
- (3) the information has not been the subject of review by the Federal courts or the Panel within the past 2 years.

(d) Agency heads shall cooperate fully with the Panel so that it can fulfill its functions in a timely and fully informed manner. The Panel shall report to the President through the National Security Advisor any instance in which it believes that an agency head is not cooperating fully with the Panel.

(e) The Panel is established for the sole purpose of advising and assisting the President in the discharge of his constitutional and discretionary authority to protect the national security of the United States. Panel decisions are committed to the discretion of the Panel, unless changed by the President.

(f) An agency head may appeal a decision of the Panel to the President through the National Security Advisor. The information shall remain classified pending a decision on the appeal.

SEC. 5.4. GENERAL RESPONSIBILITIES.

Heads of agencies that originate or handle classified information shall:

- (a) demonstrate personal commitment and commit senior management to the successful implementation of the program established under this order;
- (b) commit necessary resources to the effective implementation of the program established under this order;
- (c) ensure that agency records systems are designed and maintained to optimize the appropriate sharing and safeguarding of classified information, and to

facilitate its declassification under the terms of this order when it no longer meets the standards for continued classification; and

(d) designate a senior agency official to direct and administer the program, whose responsibilities shall include:

- (1) overseeing the agency's program established under this order, provided an agency head may designate a separate official to oversee special access programs authorized under this order. This official shall provide a full accounting of the agency's special access programs at least annually;
- (2) promulgating implementing regulations, which shall be published in the *Federal Register* to the extent that they affect members of the public;
- (3) establishing and maintaining security education and training programs;
- (4) establishing and maintaining an ongoing self-inspection program, which shall include the regular reviews of representative samples of the agency's original and derivative classification actions, and shall authorize appropriate agency officials to correct misclassification actions not covered by sections 1.7(c) and 1.7(d) of this order; and reporting annually to the Director of the Information Security Oversight Office on the agency's self-inspection program;
- (5) establishing procedures consistent with directives issued pursuant to this order to prevent unnecessary access to classified information, including procedures that:
 - (A) require that a need for access to classified information be established before initiating administrative clearance procedures; and
 - (B) ensure that the number of persons granted access to classified information meets the mission needs of the agency while also satisfying operational and security requirements and needs;
- (6) developing special contingency plans for the safeguarding of classified information used in or near hostile or potentially hostile areas;
- (7) ensuring that the performance contract or other system used to rate civilian or military personnel performance includes the designation and management of classified information as a critical element or item to be evaluated in the rating of:
 - (A) original classification authorities;
 - (B) security managers or security specialists; and
 - (C) all other personnel whose duties significantly involve the creation or handling of classified information, including

personnel who regularly apply derivative classification markings;

(8) accounting for the costs associated with the implementation of this order, which shall be reported to the Director of the Information Security Oversight Office for publication;

(9) assigning in a prompt manner agency personnel to respond to any request, appeal, challenge, complaint, or suggestion arising out of this order that pertains to classified information that originated in a component of the agency that no longer exists and for which there is no clear successor in function; and

(10) establishing a secure capability to receive information, allegations, or complaints regarding over-classification or incorrect classification within the agency and to provide guidance to personnel on proper classification as needed.

SEC. 5.5. SANCTIONS.

(a) If the Director of the Information Security Oversight Office finds that a violation of this order or its implementing directives has occurred, the Director shall make a report to the head of the agency or to the senior agency official so that corrective steps, if appropriate, may be taken.

(b) Officers and employees of the United States Government, and its contractors, licensees, certificate holders, and grantees shall be subject to appropriate sanctions if they knowingly, willfully, or negligently:

(1) disclose to unauthorized persons information properly classified under this order or predecessor orders;

(2) classify or continue the classification of information in violation of this order or any implementing directive;

(3) create or continue a special access program contrary to the requirements of this order; or

(4) contravene any other provision of this order or its implementing directives.

(c) Sanctions may include reprimand, suspension without pay, removal, termination of classification authority, loss or denial of access to classified information, or other sanctions in accordance with applicable law and agency regulation.

(d) The agency head, senior agency official, or other supervisory official shall, at a minimum, promptly remove the classification authority of any individual who demonstrates reckless disregard or a pattern of error in applying the classification standards of this order.

- (e) The agency head or senior agency official shall:
- (1) take appropriate and prompt corrective action when a violation or infraction under paragraph (b) of this section occurs; and
 - (2) notify the Director of the Information Security Oversight Office when a violation under paragraph (b)(1), (2), or (3) of this section occurs.

PART 6—GENERAL PROVISIONS

SEC. 6.1. DEFINITIONS.

For purposes of this order:

- (a) “Access” means the ability or opportunity to gain knowledge of classified information.
- (b) “Agency” means any “Executive agency,” as defined in 5 U.S.C. 105; any “Military department” as defined in 5 U.S.C. 102; and any other entity within the executive branch that comes into the possession of classified information.
- (c) “Authorized holder” of classified information means anyone who satisfies the conditions for access stated in section 4.1(a) of this order.
- (d) “Automated information system” means an assembly of computer hardware, software, or firmware configured to collect, create, communicate, compute, disseminate, process, store, or control data or information.
- (e) “Automatic declassification” means the declassification of information based solely upon:
- (1) the occurrence of a specific date or event as determined by the original classification authority; or
 - (2) the expiration of a maximum time frame for duration of classification established under this order.
- (f) “Classification” means the act or process by which information is determined to be classified information.
- (g) “Classification guidance” means any instruction or source that prescribes the classification of specific information.
- (h) “Classification guide” means a documentary form of classification guidance issued by an original classification authority that identifies the elements of information regarding a specific subject that must be classified and establishes the level and duration of classification for each such element.
- (i) “Classified national security information” or “classified information” means information that has been determined pursuant to this order or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form.
- (j) “Compilation” means an aggregation of preexisting unclassified items of information.

(k) “Confidential source” means any individual or organization that has provided, or that may reasonably be expected to provide, information to the United States on matters pertaining to the national security with the expectation that the information or relationship, or both, are to be held in confidence.

(l) “Damage to the national security” means harm to the national defense or foreign relations of the United States from the unauthorized disclosure of information, taking into consideration such aspects of the information as the sensitivity, value, utility, and provenance of that information.

(m) “Declassification” means the authorized change in the status of information from classified information to unclassified information.

(n) “Declassification guide” means written instructions issued by a declassification authority that describes the elements of information regarding a specific subject that may be declassified and the elements that must remain classified.

(o) “Derivative classification” means the incorporating, paraphrasing, restating, or generating in new form information that is already classified, and marking the newly developed material consistent with the classification markings that apply to the source information. Derivative classification includes the classification of information based on classification guidance. The duplication or reproduction of existing classified information is not derivative classification.

(p) “Document” means any recorded information, regardless of the nature of the medium or the method or circumstances of recording.

(q) “Downgrading” means a determination by a declassification authority that information classified and safeguarded at a specified level shall be classified and safeguarded at a lower level.

(r) “File series” means file units or documents arranged according to a filing system or kept together because they relate to a particular subject or function, result from the same activity, document a specific kind of transaction, take a particular physical form, or have some other relationship arising out of their creation, receipt, or use, such as restrictions on access or use.

(s) “Foreign government information” means:

(1) information provided to the United States Government by a foreign government or governments, an international organization of governments, or any element thereof, with the expectation that the information, the source of the information, or both, are to be held in confidence;

(2) information produced by the United States Government pursuant to or as a result of a joint arrangement with a foreign government or governments, or an international organization of governments, or any element thereof, requiring that the information, the arrangement, or both, are to be held in confidence; or

- (3) information received and treated as “foreign government information” under the terms of a predecessor order.
- (t) “Information” means any knowledge that can be communicated or documentary material, regardless of its physical form or characteristics, that is owned by, is produced by or for, or is under the control of the United States Government.
- (u) “Infraction” means any knowing, willful, or negligent action contrary to the requirements of this order or its implementing directives that does not constitute a “violation,” as defined below.
- (v) “Integral file block” means a distinct component of a file series, as defined in this section, that should be maintained as a separate unit in order to ensure the integrity of the records. An integral file block may consist of a set of records covering either a specific topic or a range of time, such as a Presidential administration or a 5-year retirement schedule within a specific file series that is retired from active use as a group. For purposes of automatic declassification, integral file blocks shall contain only records dated within 10 years of the oldest record in the file block.
- (w) “Integrity” means the state that exists when information is unchanged from its source and has not been accidentally or intentionally modified, altered, or destroyed.
- (x) “Intelligence” includes foreign intelligence and counterintelligence as defined by Executive Order 12333 of December 4, 1981, as amended, or by a successor order.
- (y) “Intelligence activities” means all activities that elements of the Intelligence Community are authorized to conduct pursuant to law or Executive Order 12333, as amended, or a successor order.
- (z) “Intelligence Community” means an element or agency of the U.S. Government identified in or designated pursuant to section 3(4) of the National Security Act of 1947, as amended, or section 3.5(h) of Executive Order 12333, as amended.
- (aa) “Mandatory declassification review” means the review for declassification of classified information in response to a request for declassification that meets the requirements under section 3.5 of this order.
- (bb) “Multiple sources” means two or more source documents, classification guides, or a combination of both.
- (cc) “National security” means the national defense or foreign relations of the United States.
- (dd) “Need-to-know” means a determination within the executive branch in accordance with directives issued pursuant to this order that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function.

(ee) “Network” means a system of two or more computers that can exchange data or information.

(ff) “Original classification” means an initial determination that information requires, in the interest of the national security, protection against unauthorized disclosure.

(gg) “Original classification authority” means an individual authorized in writing, either by the President, the Vice President, or by agency heads or other officials designated by the President, to classify information in the first instance.

(hh) “Records” means the records of an agency and Presidential papers or Presidential records, as those terms are defined in title 44, United States Code, including those created or maintained by a government contractor, licensee, certificate holder, or grantee that are subject to the sponsoring agency’s control under the terms of the contract, license, certificate, or grant.

(ii) “Records having permanent historical value” means Presidential papers or Presidential records and the records of an agency that the Archivist has determined should be maintained permanently in accordance with title 44, United States Code.

(jj) “Records management” means the planning, controlling, directing, organizing, training, promoting, and other managerial activities involved with respect to records creation, records maintenance and use, and records disposition in order to achieve adequate and proper documentation of the policies and transactions of the Federal Government and effective and economical management of agency operations.

(kk) “Safeguarding” means measures and controls that are prescribed to protect classified information.

(ll) “Self-inspection” means the internal review and evaluation of individual agency activities and the agency as a whole with respect to the implementation of the program established under this order and its implementing directives.

(mm) “Senior agency official” means the official designated by the agency head under section 5.4(d) of this order to direct and administer the agency’s program under which information is classified, safeguarded, and declassified.

(nn) “Source document” means an existing document that contains classified information that is incorporated, paraphrased, restated, or generated in new form into a new document.

(oo) “Special access program” means a program established for a specific class of classified information that imposes safeguarding and access requirements that exceed those normally required for information at the same classification level.

(pp) “Systematic declassification review” means the review for declassification of classified information contained in records that have been determined by the Archivist to have permanent historical value in accordance with title 44, United States Code.

(qq) “Telecommunications” means the preparation, transmission, or communication of information by electronic means.

(rr) “Unauthorized disclosure” means a communication or physical transfer of classified information to an unauthorized recipient.

(ss) “U.S. entity” includes:

- (1) State, local, or tribal governments;
- (2) State, local, and tribal law enforcement and firefighting entities;
- (3) public health and medical entities;
- (4) regional, state, local, and tribal emergency management entities, including State Adjutants General and other appropriate public safety entities; or
- (5) private sector entities serving as part of the nation’s Critical Infrastructure/ Key Resources.

(tt) “Violation” means:

- (1) any knowing, willful, or negligent action that could reasonably be expected to result in an unauthorized disclosure of classified information;
- (2) any knowing, willful, or negligent action to classify or continue the classification of information contrary to the requirements of this order or its implementing directives; or
- (3) any knowing, willful, or negligent action to create or continue a special access program contrary to the requirements of this order.

(uu) “Weapons of mass destruction” means any weapon of mass destruction as defined in 50 U.S.C. 1801(p).

SEC. 6.2. GENERAL PROVISIONS

(a) Nothing in this order shall supersede any requirement made by or under the Atomic Energy Act of 1954, as amended, or the National Security Act of 1947, as amended. “Restricted Data” and “Formerly Restricted Data” shall be handled, protected, classified, downgraded, and declassified in conformity with the provisions of the Atomic Energy Act of 1954, as amended, and regulations issued under that Act.

(b) The Director of National Intelligence may, with respect to the Intelligence Community and after consultation with the heads of affected departments and agencies, issue such policy directives and guidelines as the Director of National Intelligence deems necessary to implement this order with respect to the classification and declassification of all intelligence and intelligence-related information, and for access to and dissemination of all intelligence and intelligence-related information, both in its final form and in the form when initially gathered. Procedures or other guidance issued by Intelligence Community element heads shall be in accordance with such policy directives or guidelines issued by the Director of National Intelligence. Any such policy

directives or guidelines issued by the Director of National Intelligence shall be in accordance with directives issued by the Director of the Information Security Oversight Office under section 5.1(a) of this order.

(c) The Attorney General, upon request by the head of an agency or the Director of the Information Security Oversight Office, shall render an interpretation of this order with respect to any question arising in the course of its administration.

(d) Nothing in this order limits the protection afforded any information by other provisions of law, including the Constitution, Freedom of Information Act exemptions, the Privacy Act of 1974, and the National Security Act of 1947, as amended. This order is not intended to and does not create any right or benefit, substantive or procedural, enforceable at law by a party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person. The foregoing is in addition to the specific provisos set forth in sections 1.1(b), 3.1(c) and 5.3(e) of this order.

(e) Nothing in this order shall be construed to obligate action or otherwise affect functions by the Director of the Office of Management and Budget relating to budgetary, administrative, or legislative proposals.

(f) This order shall be implemented subject to the availability of appropriations.

(g) Executive Order 12958 of April 17, 1995, and amendments thereto, including Executive Order 13292 of March 25, 2003, are hereby revoked as of the effective date of this order.

SEC. 6.3. EFFECTIVE DATE.

This order is effective 180 days from the date of this order, except for sections 1.7, 3.3, and 3.7, which are effective immediately.

SEC. 6.4. PUBLICATION.

The Archivist of the United States shall publish this Executive Order in the *Federal Register*.

-/S/- Barack Obama
THE WHITE HOUSE,
December 29, 2009.

**EXECUTIVE ORDER 13636: IMPROVING CRITICAL INFRASTRUCTURE
CYBERSECURITY**

**EXECUTIVE ORDER 13636:
IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY**

[Signed: February 12, 2013, Federal Register Vol. 78, No. 33
(February 12, 2013)]

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

SECTION 1. POLICY.

Repeated cyber intrusions into critical infrastructure demonstrate the need for improved cybersecurity. The cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges we must confront. The national and economic security of the United States depends on the reliable functioning of the Nation's critical infrastructure in the face of such threats. It is the policy of the United States to enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties. We can achieve these goals through a partnership with the owners and operators of critical infrastructure to improve cybersecurity information sharing and collaboratively develop and implement risk-based standards.

SEC. 2. CRITICAL INFRASTRUCTURE.

As used in this order, the term critical infrastructure means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.

SEC. 3. POLICY COORDINATION.

Policy coordination, guidance, dispute resolution, and periodic in-progress reviews for the functions and programs described and assigned herein shall be provided through the interagency process established in Presidential Policy Directive-1 of February 13, 2009 (Organization of the National Security Council System), or any successor.

SEC. 4. CYBERSECURITY INFORMATION SHARING.

(a) It is the policy of the United States Government to increase the volume, timeliness, and quality of cyber threat information shared with U.S. private

**EXECUTIVE ORDER 13636: IMPROVING CRITICAL INFRASTRUCTURE
CYBERSECURITY**

sector entities so that these entities may better protect and defend themselves against cyber threats. Within 120 days of the date of this order, the Attorney General, the Secretary of Homeland Security (the “Secretary”), and the Director of National Intelligence shall each issue instructions consistent with their authorities and with the requirements of section 12(c) of this order to ensure the timely production of unclassified reports of cyber threats to the U.S. homeland that identify a specific targeted entity. The instructions shall address the need to protect intelligence and law enforcement sources, methods, operations, and investigations.

(b) The Secretary and the Attorney General, in coordination with the Director of National Intelligence, shall establish a process that rapidly disseminates the reports produced pursuant to section 4(a) of this order to the targeted entity. Such process shall also, consistent with the need to protect national security information, include the dissemination of classified reports to critical infrastructure entities authorized to receive them. The Secretary and the Attorney General, in coordination with the Director of National Intelligence, shall establish a system for tracking the production, dissemination, and disposition of these reports.

(c) To assist the owners and operators of critical infrastructure in protecting their systems from unauthorized access, exploitation, or harm, the Secretary, consistent with 6 U.S.C. 143 and in collaboration with the Secretary of Defense, shall, within 120 days of the date of this order, establish procedures to expand the Enhanced Cybersecurity Services program to all critical infrastructure sectors. This voluntary information sharing program will provide classified cyber threat and technical information from the Government to eligible critical infrastructure companies or commercial service providers that offer security services to critical infrastructure.

(d) The Secretary, as the Executive Agent for the Classified National Security Information Program created under Executive Order 13549 of August 18, 2010 (Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities), shall expedite the processing of security clearances to appropriate personnel employed by critical infrastructure owners and operators, prioritizing the critical infrastructure identified in section 9 of this order.

(e) In order to maximize the utility of cyber threat information sharing with the private sector, the Secretary shall expand the use of programs that bring private sector subject-matter experts into Federal service on a temporary basis. These subject matter experts should provide advice regarding the content, structure, and types of information most useful to critical infrastructure owners and operators in reducing and mitigating cyber risks.

**EXECUTIVE ORDER 13636: IMPROVING CRITICAL INFRASTRUCTURE
CYBERSECURITY**

SEC. 5. PRIVACY AND CIVIL LIBERTIES PROTECTIONS.

(a) Agencies shall coordinate their activities under this order with their senior agency officials for privacy and civil liberties and ensure that privacy and civil liberties protections are incorporated into such activities. Such protections shall be based upon the Fair Information Practice Principles and other privacy and civil liberties policies, principles, and frameworks as they apply to each agency's activities.

(b) The Chief Privacy Officer and the Officer for Civil Rights and Civil Liberties of the Department of Homeland Security (DHS) shall assess the privacy and civil liberties risks of the functions and programs undertaken by DHS as called for in this order and shall recommend to the Secretary ways to minimize or mitigate such risks, in a publicly available report, to be released within 1 year of the date of this order. Senior agency privacy and civil liberties officials for other agencies engaged in activities under this order shall conduct assessments of their agency activities and provide those assessments to DHS for consideration and inclusion in the report. The report shall be reviewed on an annual basis and revised as necessary. The report may contain a classified annex if necessary. Assessments shall include evaluation of activities against the Fair Information Practice Principles and other applicable privacy and civil liberties policies, principles, and frameworks. Agencies shall consider the assessments and recommendations of the report in implementing privacy and civil liberties protections for agency activities.

(c) In producing the report required under subsection (b) of this section, the Chief Privacy Officer and the Officer for Civil Rights and Civil Liberties of DHS shall consult with the Privacy and Civil Liberties Oversight Board and coordinate with the Office of Management and Budget (OMB).

(d) Information submitted voluntarily in accordance with 6 U.S.C. 133 by private entities under this order shall be protected from disclosure to the fullest extent permitted by law.

SEC. 6. CONSULTATIVE PROCESS.

The Secretary shall establish a consultative process to coordinate improvements to the cybersecurity of critical infrastructure. As part of the consultative process, the Secretary shall engage and consider the advice, on matters set forth in this order, of the Critical Infrastructure Partnership Advisory Council; Sector Coordinating Councils; critical infrastructure owners and operators; Sector-Specific Agencies; other relevant agencies; independent regulatory agencies; State, local, territorial, and tribal governments; universities; and outside experts.

**EXECUTIVE ORDER 13636: IMPROVING CRITICAL INFRASTRUCTURE
CYBERSECURITY**

SEC. 7. BASELINE FRAMEWORK TO REDUCE CYBER RISK TO CRITICAL INFRASTRUCTURE.

(a) The Secretary of Commerce shall direct the Director of the National Institute of Standards and Technology (the “Director”) to lead the development of a framework to reduce cyber risks to critical infrastructure (the “Cybersecurity Framework”). The Cybersecurity Framework shall include a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks. The Cybersecurity Framework shall incorporate voluntary consensus standards and industry best practices to the fullest extent possible. The Cybersecurity Framework shall be consistent with voluntary international standards when such international standards will advance the objectives of this order, and shall meet the requirements of the National Institute of Standards and Technology Act, as amended (15 U.S.C. 271 et seq.), the National Technology Transfer and Advancement Act of 1995 (Public Law 104-113), and OMB Circular A-119, as revised.

(b) The Cybersecurity Framework shall provide a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls, to help owners and operators of critical infrastructure identify, assess, and manage cyber risk. The Cybersecurity Framework shall focus on identifying cross-sector security standards and guidelines applicable to critical infrastructure. The Cybersecurity Framework will also identify areas for improvement that should be addressed through future collaboration with particular sectors and standards-developing organizations. To enable technical innovation and account for organizational differences, the Cybersecurity Framework will provide guidance that is technology neutral and that enables critical infrastructure sectors to benefit from a competitive market for products and services that meet the standards, methodologies, procedures, and processes developed to address cyber risks. The Cybersecurity Framework shall include guidance for measuring the performance of an entity in implementing the Cybersecurity Framework.

(c) The Cybersecurity Framework shall include methodologies to identify and mitigate impacts of the Cybersecurity Framework and associated information security measures or controls on business confidentiality, and to protect individual privacy and civil liberties.

(d) In developing the Cybersecurity Framework, the Director shall engage in an open public review and comment process. The Director shall also consult with the Secretary, the National Security Agency, Sector-Specific Agencies and other interested agencies including OMB, owners and operators of critical infrastructure, and other stakeholders through the consultative process

**EXECUTIVE ORDER 13636: IMPROVING CRITICAL INFRASTRUCTURE
CYBERSECURITY**

established in section 6 of this order. The Secretary, the Director of National Intelligence, and the heads of other relevant agencies shall provide threat and vulnerability information and technical expertise to inform the development of the Cybersecurity Framework. The Secretary shall provide performance goals for the Cybersecurity Framework informed by work under section 9 of this order.

(e) Within 240 days of the date of this order, the Director shall publish a preliminary version of the Cybersecurity Framework (the “preliminary Framework”). Within 1 year of the date of this order, and after coordination with the Secretary to ensure suitability under section 8 of this order, the Director shall publish a final version of the Cybersecurity Framework (the “final Framework”).

(f) Consistent with statutory responsibilities, the Director will ensure the Cybersecurity Framework and related guidance is reviewed and updated as necessary, taking into consideration technological changes, changes in cyber risks, operational feedback from owners and operators of critical infrastructure, experience from the implementation of section 8 of this order, and any other relevant factors.

SEC. 8. VOLUNTARY CRITICAL INFRASTRUCTURE CYBERSECURITY PROGRAM.

(a) The Secretary, in coordination with Sector-Specific Agencies, shall establish a voluntary program to support the adoption of the Cybersecurity Framework by owners and operators of critical infrastructure and any other interested entities (the “Program”).

(b) Sector-Specific Agencies, in consultation with the Secretary and other interested agencies, shall coordinate with the Sector Coordinating Councils to review the Cybersecurity Framework and, if necessary, develop implementation guidance or supplemental materials to address sector-specific risks and operating environments.

(c) Sector-Specific Agencies shall report annually to the President, through the Secretary, on the extent to which owners and operators notified under section 9 of this order are participating in the Program.

(d) The Secretary shall coordinate establishment of a set of incentives designed to promote participation in the Program. Within 120 days of the date of this order, the Secretary and the Secretaries of the Treasury and Commerce each shall make recommendations separately to the President, through the Assistant to the President for Homeland Security and Counterterrorism and the Assistant to the President for Economic Affairs, that shall include analysis of the benefits and relative effectiveness of such incentives, and whether the incentives would

**EXECUTIVE ORDER 13636: IMPROVING CRITICAL INFRASTRUCTURE
CYBERSECURITY**

require legislation or can be provided under existing law and authorities to participants in the Program.

(e) Within 120 days of the date of this order, the Secretary of Defense and the Administrator of General Services, in consultation with the Secretary and the Federal Acquisition Regulatory Council, shall make recommendations to the President, through the Assistant to the President for Homeland Security and Counterterrorism and the Assistant to the President for Economic Affairs, on the feasibility, security benefits, and relative merits of incorporating security standards into acquisition planning and contract administration. The report shall address what steps can be taken to harmonize and make consistent existing procurement requirements related to cybersecurity.

SEC. 9. IDENTIFICATION OF CRITICAL INFRASTRUCTURE AT GREATEST RISK.

(a) Within 150 days of the date of this order, the Secretary shall use a risk-based approach to identify critical infrastructure where a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security. In identifying critical infrastructure for this purpose, the Secretary shall use the consultative process established in section 6 of this order and draw upon the expertise of Sector-Specific Agencies. The Secretary shall apply consistent, objective criteria in identifying such critical infrastructure. The Secretary shall not identify any commercial information technology products or consumer information technology services under this section. The Secretary shall review and update the list of identified critical infrastructure under this section on an annual basis, and provide such list to the President, through the Assistant to the President for Homeland Security and Counterterrorism and the Assistant to the President for Economic Affairs.

(b) Heads of Sector-Specific Agencies and other relevant agencies shall provide the Secretary with information necessary to carry out the responsibilities under this section. The Secretary shall develop a process for other relevant stakeholders to submit information to assist in making the identifications required in subsection (a) of this section.

(c) The Secretary, in coordination with Sector-Specific Agencies, shall confidentially notify owners and operators of critical infrastructure identified under subsection (a) of this section that they have been so identified, and ensure identified owners and operators are provided the basis for the determination. The Secretary shall establish a process through which owners and operators of critical infrastructure may submit relevant information and request reconsideration of identifications under subsection (a) of this section.

**EXECUTIVE ORDER 13636: IMPROVING CRITICAL INFRASTRUCTURE
CYBERSECURITY**

SEC. 10. ADOPTION OF FRAMEWORK.

(a) Agencies with responsibility for regulating the security of critical infrastructure shall engage in a consultative process with DHS, OMB, and the National Security Staff to review the preliminary Cybersecurity Framework and determine if current cybersecurity regulatory requirements are sufficient given current and projected risks. In making such determination, these agencies shall consider the identification of critical infrastructure required under section 9 of this order. Within 90 days of the publication of the preliminary Framework, these agencies shall submit a report to the President, through the Assistant to the President for Homeland Security and Counterterrorism, the Director of OMB, and the Assistant to the President for Economic Affairs, that states whether or not the agency has clear authority to establish requirements based upon the Cybersecurity Framework to sufficiently address current and projected cyber risks to critical infrastructure, the existing authorities identified, and any additional authority required.

(b) If current regulatory requirements are deemed to be insufficient, within 90 days of publication of the final Framework, agencies identified in subsection (a) of this section shall propose prioritized, risk-based, efficient, and coordinated actions, consistent with Executive Order 12866 of September 30, 1993 (Regulatory Planning and Review), Executive Order 13563 of January 18, 2011 (Improving Regulation and Regulatory Review), and Executive Order 13609 of May 1, 2012 (Promoting International Regulatory Cooperation), to mitigate cyber risk.

(c) Within 2 years after publication of the final Framework, consistent with Executive Order 13563 and Executive Order 13610 of May 10, 2012 (Identifying and Reducing Regulatory Burdens), agencies identified in subsection (a) of this section shall, in consultation with owners and operators of critical infrastructure, report to OMB on any critical infrastructure subject to ineffective, conflicting, or excessively burdensome cybersecurity requirements. This report shall describe efforts made by agencies, and make recommendations for further actions, to minimize or eliminate such requirements.

(d) The Secretary shall coordinate the provision of technical assistance to agencies identified in subsection (a) of this section on the development of their cybersecurity workforce and programs.

(e) Independent regulatory agencies with responsibility for regulating the security of critical infrastructure are encouraged to engage in a consultative process with the Secretary, relevant Sector-Specific Agencies, and other affected parties to consider prioritized actions to mitigate cyber risks for critical infrastructure consistent with their authorities.

**EXECUTIVE ORDER 13636: IMPROVING CRITICAL INFRASTRUCTURE
CYBERSECURITY**

SEC. 11. DEFINITIONS.

- (a) “Agency” means any authority of the United States that is an “agency” under 44 U.S.C. 3502(1), other than those considered to be independent regulatory agencies, as defined in 44 U.S.C. 3502(5).
- (b) “Critical Infrastructure Partnership Advisory Council” means the council established by DHS under 6 U.S.C. 451 to facilitate effective interaction and coordination of critical infrastructure protection activities among the Federal Government; the private sector; and State, local, territorial, and tribal governments.
- (c) “Fair Information Practice Principles” means the eight principles set forth in Appendix A of the National Strategy for Trusted Identities in Cyberspace.
- (d) “Independent regulatory agency” has the meaning given the term in 44 U.S.C. 3502(5).
- (e) “Sector Coordinating Council” means a private sector coordinating council composed of representatives of owners and operators within a particular sector of critical infrastructure established by the National Infrastructure Protection Plan or any successor.
- (f) “Sector-Specific Agency” has the meaning given the term in Presidential Policy Directive-21 of February 12, 2013 (Critical Infrastructure Security and Resilience), or any successor.

SEC. 12. GENERAL PROVISIONS.

- (a) This order shall be implemented consistent with applicable law and subject to the availability of appropriations. Nothing in this order shall be construed to provide an agency with authority for regulating the security of critical infrastructure in addition to or to a greater extent than the authority the agency has under existing law. Nothing in this order shall be construed to alter or limit any authority or responsibility of an agency under existing law.
- (b) Nothing in this order shall be construed to impair or otherwise affect the functions of the Director of OMB relating to budgetary, administrative, or legislative proposals.
- (c) All actions taken pursuant to this order shall be consistent with requirements and authorities to protect intelligence and law enforcement sources and methods. Nothing in this order shall be interpreted to supersede measures established under authority of law to protect the security and integrity of specific activities and associations that are in direct support of intelligence and law enforcement operations.
- (d) This order shall be implemented consistent with U.S. international obligations.

**EXECUTIVE ORDER 13636: IMPROVING CRITICAL INFRASTRUCTURE
CYBERSECURITY**

(e) This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

-/S/- Barack Obama
THE WHITE HOUSE,
February 12, 2013.

**EXECUTIVE ORDER 14086: ENHANCING SAFEGUARDS FOR UNITED STATES
SIGNALS INTELLIGENCE ACTIVITIES**

**EXECUTIVE ORDER 14086: ENHANCING SAFEGUARDS FOR UNITED STATES
SIGNALS INTELLIGENCE ACTIVITIES**

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. *Purpose.* The United States collects signals intelligence so that its national security decisionmakers have access to the timely, accurate, and insightful information necessary to advance the national security interests of the United States and to protect its citizens and the citizens of its allies and partners from harm. Signals intelligence capabilities are a major reason we have been able to adapt to a dynamic and challenging security environment, and the United States must preserve and continue to develop robust and technologically advanced signals intelligence capabilities to protect our security and that of our allies and partners. At the same time, the United States recognizes that signals intelligence activities must take into account that all persons should be treated with dignity and respect, regardless of their nationality or wherever they might reside, and that all persons have legitimate privacy interests in the handling of their personal information. Therefore, this order establishes safeguards for such signals intelligence activities.

Sec. 2. *Signals Intelligence Activities.*

(a) Principles. Signals intelligence activities shall be authorized and conducted consistent with the following principles:

(i) Signals intelligence activities shall be authorized by statute or by Executive Order, proclamation, or other Presidential directive and undertaken in accordance with the Constitution and with applicable statutes and Executive Orders, proclamations, and other Presidential directives.

(ii) Signals intelligence activities shall be subject to appropriate safeguards, which shall ensure that privacy and civil liberties are integral considerations in the planning and implementation of such activities so that:

(A) signals intelligence activities shall be conducted only following a determination, based on a reasonable assessment of all relevant factors, that the activities are necessary to advance a validated intelligence priority, although signals intelligence does not have to be the sole means available or used for advancing aspects of the validated intelligence priority; and

**EXECUTIVE ORDER 14086: ENHANCING SAFEGUARDS FOR UNITED STATES
SIGNALS INTELLIGENCE ACTIVITIES**

(B) signals intelligence activities shall be conducted only to the extent and in a manner that is proportionate to the validated intelligence priority for which they have been authorized, with the aim of achieving a proper balance between the importance of the validated intelligence priority being advanced and the impact on the privacy and civil liberties of all persons, regardless of their nationality or wherever they might reside.

(iii) Signals intelligence activities shall be subjected to rigorous oversight in order to ensure that they comport with the principles identified above.

(b) Objectives. Signals intelligence collection activities shall be conducted in pursuit of legitimate objectives.

(i) Legitimate objectives.

(A) Signals intelligence collection activities shall be conducted only in pursuit of one or more of the following objectives:

- (1) understanding or assessing the capabilities, intentions, or activities of a foreign government, a foreign military, a faction of a foreign nation, a foreign-based political organization, or an entity acting on behalf of or controlled by any such foreign government, military, faction, or political organization, in order to protect the national security of the United States and of its allies and partners;
- (2) understanding or assessing the capabilities, intentions, or activities of foreign organizations, including international terrorist organizations, that pose a current or potential threat to the national security of the United States or of its allies or partners;
- (3) understanding or assessing transnational threats that impact global security, including climate and other ecological change, public health risks, humanitarian threats, political instability, and geographic rivalry;
- (4) protecting against foreign military capabilities and activities;
- (5) protecting against terrorism, the taking of hostages, and the holding of individuals captive (including the identification, location, and rescue of hostages and captives) conducted by or on behalf of a foreign government, foreign organization, or foreign person;
- (6) protecting against espionage, sabotage, assassination, or other intelligence activities conducted by, on behalf of, or with the assistance of a foreign government, foreign organization, or foreign person;
- (7) protecting against threats from the development, possession, or proliferation of weapons of mass destruction or related technologies

**EXECUTIVE ORDER 14086: ENHANCING SAFEGUARDS FOR UNITED STATES
SIGNALS INTELLIGENCE ACTIVITIES**

and threats conducted by, on behalf of, or with the assistance of a foreign government, foreign organization, or foreign person;

(8) protecting against cybersecurity threats created or exploited by, or malicious cyber activities conducted by or on behalf of, a foreign government, foreign organization, or foreign person;

(9) protecting against threats to the personnel of the United States or of its allies or partners;

(10) protecting against transnational criminal threats, including illicit finance and sanctions evasion related to one or more of the other objectives identified in subsection (b)(i) of this section;

(11) protecting the integrity of elections and political processes, government property, and United States infrastructure (both physical and electronic) from activities conducted by, on behalf of, or with the assistance of a foreign government, foreign organization, or foreign person; and

(12) advancing collection or operational capabilities or activities in order to further a legitimate objective identified in subsection (b)(i) of this section.

(B) The President may authorize updates to the list of objectives in light of new national security imperatives, such as new or heightened threats to the national security of the United States, for which the President determines that signals intelligence collection activities may be used. The Director of National Intelligence (Director) shall publicly release any updates to the list of objectives authorized by the President, unless the President determines that doing so would pose a risk to the national security of the United States.

(ii) Prohibited objectives.

(A) Signals intelligence collection activities shall not be conducted for the purpose of:

(1) suppressing or burdening criticism, dissent, or the free expression of ideas or political opinions by individuals or the press;

(2) suppressing or restricting legitimate privacy interests;

(3) suppressing or restricting a right to legal counsel; or

(4) disadvantaging persons based on their ethnicity, race, gender, gender identity, sexual orientation, or religion.

(B) It is not a legitimate objective to collect foreign private commercial information or trade secrets to afford a competitive advantage to United States companies and United States business sectors commercially. The collection of such information is authorized only to

EXECUTIVE ORDER 14086: ENHANCING SAFEGUARDS FOR UNITED STATES SIGNALS INTELLIGENCE ACTIVITIES

protect the national security of the United States or of its allies or partners.

(iii) Validation of signals intelligence collection priorities.

(A) Under section 102A of the National Security Act of 1947, as amended (50 U.S.C. 3024), the Director must establish priorities for the Intelligence Community to ensure the timely and effective collection of national intelligence, including national intelligence collected through signals intelligence. The Director does this through the National Intelligence Priorities Framework (NIPF), which the Director maintains and presents to the President, through the Assistant to the President for National Security Affairs, on a regular basis. In order to ensure that signals intelligence collection activities are undertaken to advance legitimate objectives, before presenting the NIPF or any successor framework that identifies intelligence priorities to the President, the Director shall obtain from the Civil Liberties Protection Officer of the Office of the Director of National Intelligence (CLPO) an assessment as to whether, with regard to anticipated signals intelligence collection activities, each of the intelligence priorities identified in the NIPF or successor framework:

- (1) advances one or more of the legitimate objectives set forth in subsection (b)(i) of this section;
- (2) neither was designed nor is anticipated to result in signals intelligence collection in contravention of the prohibited objectives set forth in subsection (b)(ii) of this section; and
- (3) was established after appropriate consideration for the privacy and civil liberties of all persons, regardless of their nationality or wherever they might reside.

(B) If the Director disagrees with any aspect of the CLPO's assessment with respect to any of the intelligence priorities identified in the NIPF or successor framework, the Director shall include the CLPO's assessment and the Director's views when presenting the NIPF to the President.

(c) Privacy and civil liberties safeguards. The following safeguards shall fulfill the principles contained in subsections (a)(ii) and (a)(iii) of this section.

(i) Collection of signals intelligence.

(A) The United States shall conduct signals intelligence collection activities only following a determination that a specific signals intelligence collection activity, based on a reasonable assessment of all relevant factors, is necessary to advance a validated intelligence

**EXECUTIVE ORDER 14086: ENHANCING SAFEGUARDS FOR UNITED STATES
SIGNALS INTELLIGENCE ACTIVITIES**

priority, although signals intelligence does not have to be the sole means available or used for advancing aspects of the validated intelligence priority; it could be used, for example, to ensure alternative pathways for validation or for maintaining reliable access to the same information. In determining whether to collect signals intelligence consistent with this principle, the United States—through an element of the Intelligence Community or through an interagency committee consisting in whole or in part of the heads of elements of the Intelligence Community, the heads of departments containing such elements, or their designees—shall consider the availability, feasibility, and appropriateness of other less intrusive sources and methods for collecting the information necessary to advance a validated intelligence priority, including from diplomatic and public sources, and shall prioritize such available, feasible, and appropriate alternatives to signals intelligence.

(B) Signals intelligence collection activities shall be as tailored as feasible to advance a validated intelligence priority and, taking due account of relevant factors, not disproportionately impact privacy and civil liberties. Such factors may include, depending on the circumstances, the nature of the pursued objective; the feasible steps taken to limit the scope of the collection to the authorized purpose; the intrusiveness of the collection activity, including its duration; the probable contribution of the collection to the objective pursued; the reasonably foreseeable consequences to individuals, including unintended third parties; the nature and sensitivity of the data to be collected; and the safeguards afforded to the information collected.

(C) For purposes of subsection (c)(i) of this section, the scope of a specific signals intelligence collection activity may include, for example, a specific line of effort or target, as appropriate.

(ii) Bulk collection of signals intelligence.

(A) Targeted collection shall be prioritized. The bulk collection of signals intelligence shall be authorized only based on a determination—by an element of the Intelligence Community or through an interagency committee consisting in whole or in part of the heads of elements of the Intelligence Community, the heads of departments containing such elements, or their designees—that the information necessary to advance a validated intelligence priority cannot reasonably be obtained by targeted collection. When it is determined to be necessary to engage in bulk collection in order to advance a validated intelligence priority, the element of the

**EXECUTIVE ORDER 14086: ENHANCING SAFEGUARDS FOR UNITED STATES
SIGNALS INTELLIGENCE ACTIVITIES**

Intelligence Community shall apply reasonable methods and technical measures in order to limit the data collected to only what is necessary to advance a validated intelligence priority, while minimizing the collection of non-pertinent information.

(B) Each element of the Intelligence Community that collects signals intelligence through bulk collection shall use such information only in pursuit of one or more of the following objectives:

- (1) protecting against terrorism, the taking of hostages, and the holding of individuals captive (including the identification, location, and rescue of hostages and captives) conducted by or on behalf of a foreign government, foreign organization, or foreign person;
- (2) protecting against espionage, sabotage, assassination, or other intelligence activities conducted by, on behalf of, or with the assistance of a foreign government, foreign organization, or foreign person;
- (3) protecting against threats from the development, possession, or proliferation of weapons of mass destruction or related technologies and threats conducted by, on behalf of, or with the assistance of a foreign government, foreign organization, or foreign person;
- (4) protecting against cybersecurity threats created or exploited by, or malicious cyber activities conducted by or on behalf of, a foreign government, foreign organization, or foreign person;
- (5) protecting against threats to the personnel of the United States or of its allies or partners; and
- (6) protecting against transnational criminal threats, including illicit finance and sanctions evasion related to one or more of the other objectives identified in subsection (c)(ii) of this section.

(C) The President may authorize updates to the list of objectives in light of new national security imperatives, such as new or heightened threats to the national security of the United States, for which the President determines that bulk collection may be used. The Director shall publicly release any updates to the list of objectives authorized by the President, unless the President determines that doing so would pose a risk to the national security of the United States.

(D) In order to minimize any impact on privacy and civil liberties, a targeted signals intelligence collection activity that temporarily uses data acquired without discriminants (for example, without specific

**EXECUTIVE ORDER 14086: ENHANCING SAFEGUARDS FOR UNITED STATES
SIGNALS INTELLIGENCE ACTIVITIES**

identifiers or selection terms) shall be subject to the safeguards described in this subsection, unless such data is:

- (1) used only to support the initial technical phase of the targeted signals intelligence collection activity;
- (2) retained for only the short period of time required to complete this phase; and
- (3) thereafter deleted.

(iii) Handling of personal information collected through signals intelligence.

(A) **Minimization.** Each element of the Intelligence Community that handles personal information collected through signals intelligence shall establish and apply policies and procedures designed to minimize the dissemination and retention of personal information collected through signals intelligence.

(1) **Dissemination.** Each element of the Intelligence Community that handles personal information collected through signals intelligence:

- (a) shall disseminate non-United States persons' personal information collected through signals intelligence only if it involves one or more of the comparable types of information that section 2.3 of Executive Order 12333 of December 4, 1981 (United States Intelligence Activities), as amended, states may be disseminated in the case of information concerning United States persons;
- (b) shall not disseminate personal information collected through signals intelligence solely because of a person's nationality or country of residence;
- (c) shall disseminate within the United States Government personal information collected through signals intelligence only if an authorized and appropriately trained individual has a reasonable belief that the personal information will be appropriately protected and that the recipient has a need to know the information;
- (d) shall take due account of the purpose of the dissemination, the nature and extent of the personal information being disseminated, and the potential for harmful impact on the person or persons concerned before disseminating personal information collected through signals intelligence to recipients outside the United States

EXECUTIVE ORDER 14086: ENHANCING SAFEGUARDS FOR UNITED STATES SIGNALS INTELLIGENCE ACTIVITIES

Government, including to a foreign government or international organization; and

(e) shall not disseminate personal information collected through signals intelligence for the purpose of circumventing the provisions of this order.

(2) Retention. Each element of the Intelligence Community that handles personal information collected through signals intelligence:

(a) shall retain non-United States persons' personal information collected through signals intelligence only if the retention of comparable information concerning United States persons would be permitted under applicable law and shall subject such information to the same retention periods that would apply to comparable information concerning United States persons;

(b) shall subject non-United States persons' personal information collected through signals intelligence for which no final retention determination has been made to the same temporary retention periods that would apply to comparable information concerning United States persons; and

(c) shall delete non-United States persons' personal information collected through signals intelligence that may no longer be retained in the same manner that comparable information concerning United States persons would be deleted.

(B) Data security and access. Each element of the Intelligence Community that handles personal information collected through signals intelligence:

(1) shall process and store personal information collected through signals intelligence under conditions that provide appropriate protection and prevent access by unauthorized persons, consistent with the applicable safeguards for sensitive information contained in relevant Executive Orders, proclamations, other Presidential directives, Intelligence Community directives, and associated policies;

(2) shall limit access to such personal information to authorized personnel who have a need to know the information to perform their mission and have received appropriate training on the requirements of applicable United States law, as described in

**EXECUTIVE ORDER 14086: ENHANCING SAFEGUARDS FOR UNITED STATES
SIGNALS INTELLIGENCE ACTIVITIES**

policies and procedures issued under subsection (c)(iv) of this section; and

(3) shall ensure that personal information collected through signals intelligence for which no final retention determination has been made is accessed only in order to make or support such a determination or to conduct authorized administrative, testing, development, security, or oversight functions.

(C) Data quality. Each element of the Intelligence Community that handles personal information collected through signals intelligence shall include such personal information in intelligence products only as consistent with applicable Intelligence Community standards for accuracy and objectivity, with a focus on applying standards relating to the quality and reliability of the information, consideration of alternative sources of information and interpretations of data, and objectivity in performing analysis.

(D) Queries of bulk collection. Each element of the Intelligence Community that conducts queries of unminimized signals intelligence obtained by bulk collection shall do so consistent with the permissible uses of signals intelligence obtained by bulk collection identified in subsection (c)(ii)(B) of this section and according to policies and procedures issued under subsection (c)(iv) of this section, which shall appropriately take into account the impact on the privacy and civil liberties of all persons, regardless of their nationality or wherever they might reside.

(E) Documentation. In order to facilitate the oversight processes set forth in subsection (d) of this section and the redress mechanism set forth in section 3 of this order, each element of the Intelligence Community that engages in signals intelligence collection activities shall maintain documentation to the extent reasonable in light of the nature and type of collection at issue and the context in which it is collected. The content of any such documentation may vary based on the circumstances but shall, to the extent reasonable, provide the factual basis pursuant to which the element of the Intelligence Community, based on a reasonable assessment of all relevant factors, assesses that the signals intelligence collection activity is necessary to advance a validated intelligence priority.

(iv) Update and publication of policies and procedures. The head of each element of the Intelligence Community:

(A) shall continue to use the policies and procedures issued pursuant to Presidential Policy Directive 28 of January 17, 2014 (Signals

**EXECUTIVE ORDER 14086: ENHANCING SAFEGUARDS FOR UNITED STATES
SIGNALS INTELLIGENCE ACTIVITIES**

Intelligence Activities) (PPD–28), until they are updated pursuant to subsection (c)(iv)(B) of this section;

(B) shall, within 1 year of the date of this order, in consultation with the Attorney General, the CLPO, and the Privacy and Civil Liberties Oversight Board (PCLOB), update those policies and procedures as necessary to implement the privacy and civil liberties safeguards in this order; and

(C) shall, within 1 year of the date of this order, release these policies and procedures publicly to the maximum extent possible, consistent with the protection of intelligence sources and methods, in order to enhance the public’s understanding of, and to promote public trust in, the safeguards pursuant to which the United States conducts signals intelligence activities.

(v) Review by the PCLOB.

(A) Nature of review. Consistent with applicable law, the PCLOB is encouraged to conduct a review of the updated policies and procedures described in subsection (c)(iv)(B) of this section once they have been issued to ensure that they are consistent with the enhanced safeguards contained in this order.

(B) Consideration of review. Within 180 days of completion of any review by the PCLOB described in subsection (c)(v)(A) of this section, the head of each element of the Intelligence Community shall carefully consider and shall implement or otherwise address all recommendations contained in such review, consistent with applicable law.

(d) Subjecting signals intelligence activities to rigorous oversight. The actions directed in this subsection are designed to build on the oversight mechanisms that elements of the Intelligence Community already have in place, in order to further ensure that signals intelligence activities are subjected to rigorous oversight.

(i) Legal, oversight, and compliance officials. Each element of the Intelligence Community that collects signals intelligence:

(A) shall have in place senior-level legal, oversight, and compliance officials who conduct periodic oversight of signals intelligence activities, including an Inspector General, a Privacy and Civil Liberties Officer, and an officer or officers in a designated compliance role with the authority to conduct oversight of and ensure compliance with applicable United States law;

(B) shall provide such legal, oversight, and compliance officials access to all information pertinent to carrying out their oversight

EXECUTIVE ORDER 14086: ENHANCING SAFEGUARDS FOR UNITED STATES SIGNALS INTELLIGENCE ACTIVITIES

responsibilities under this subsection, consistent with the protection of intelligence sources or methods, including their oversight responsibilities to ensure that any appropriate actions are taken to remediate an incident of non-compliance with applicable United States law; and

(C) shall not take any actions designed to impede or improperly influence such legal, oversight, and compliance officials in carrying out their oversight responsibilities under this subsection.

(ii) Training. Each element of the Intelligence Community shall maintain appropriate training requirements to ensure that all employees with access to signals intelligence know and understand the requirements of this order and the policies and procedures for reporting and remediating incidents of non-compliance with applicable United States law.

(iii) Significant incidents of non-compliance.

(A) Each element of the Intelligence Community shall ensure that, if a legal, oversight, or compliance official, as described in subsection (d)(i) of this section, or any other employee, identifies a significant incident of non-compliance with applicable United States law, the incident is reported promptly to the head of the element of the Intelligence Community, the head of the executive department or agency (agency) containing the element of the Intelligence Community (to the extent relevant), and the Director.

(B) Upon receipt of such report, the head of the element of the Intelligence Community, the head of the agency containing the element of the Intelligence Community (to the extent relevant), and the Director shall ensure that any necessary actions are taken to remediate and prevent the recurrence of the significant incident of non-compliance.

(e) Savings clause. Provided the signals intelligence collection is conducted consistent with and in the manner prescribed by this section of this order, this order does not limit any signals intelligence collection technique authorized under the National Security Act of 1947, as amended (50 U.S.C. 3001 et seq.), the Foreign Intelligence Surveillance Act of 1978, as amended (50 U.S.C. 1801 et seq.) (FISA), Executive Order 12333, or other applicable law or Presidential directive.

Sec. 3. Signals Intelligence Redress Mechanism.

(a) Purpose. This section establishes a redress mechanism to review qualifying complaints transmitted by the appropriate public authority in a qualifying state concerning United States signals intelligence activities for

EXECUTIVE ORDER 14086: ENHANCING SAFEGUARDS FOR UNITED STATES SIGNALS INTELLIGENCE ACTIVITIES

any covered violation of United States law and, if necessary, appropriate remediation.

(b) Process for submission of qualifying complaints. Within 60 days of the date of this order, the Director, in consultation with the Attorney General and the heads of elements of the Intelligence Community that collect or handle personal information collected through signals intelligence, shall establish a process for the submission of qualifying complaints transmitted by the appropriate public authority in a qualifying state.

(c) Initial investigation of qualifying complaints by the CLPO.

(i) Establishment. The Director, in consultation with the Attorney General, shall establish a process that authorizes the CLPO to investigate, review, and, as necessary, order appropriate remediation for qualifying complaints. This process shall govern how the CLPO will review qualifying complaints in a manner that protects classified or otherwise privileged or protected information and shall ensure, at a minimum, that for each qualifying complaint the CLPO shall:

(A) review information necessary to investigate the qualifying complaint;

(B) exercise its statutory and delegated authority to determine whether there was a covered violation by:

(i) taking into account both relevant national security interests and applicable privacy protections;

(ii) giving appropriate deference to any relevant determinations made by national security officials; and

(iii) applying the law impartially;¹

(C) determine the appropriate remediation for any covered violation;

(D) provide a classified report on information indicating a violation of any authority subject to the oversight of the Foreign Intelligence Surveillance Court (FISC) to the Assistant Attorney General for National Security, who shall report violations to the FISC in accordance with its rules of procedure;

(E) after the review is completed, inform the complainant, through the appropriate public authority in a qualifying state and without confirming or denying that the complainant was subject to United States signals intelligence activities, that:

(1) “the review either did not identify any covered violations or the Civil Liberties Protection Officer of the Office of the

¹ Above mirrors subparagraph numbering as contained in the EO

**EXECUTIVE ORDER 14086: ENHANCING SAFEGUARDS FOR UNITED STATES
SIGNALS INTELLIGENCE ACTIVITIES**

Director of National Intelligence issued a determination requiring appropriate remediation”;

(2) the complainant or an element of the Intelligence Community may, as prescribed in the regulations issued by the Attorney General pursuant to section 3(d)(i) of this order, apply for review of the CLPO’s determinations by the Data Protection Review Court described in subsection (d) of this section; and

(3) if either the complainant or an element of the Intelligence Community applies for review by the Data Protection Review Court, a special advocate will be selected by the Data Protection Review Court to advocate regarding the complainant’s interest in the matter;

(F) maintain appropriate documentation of its review of the qualifying complaint and produce a classified decision explaining the basis for its factual findings, determination with respect to whether a covered violation occurred, and determination of the appropriate remediation in the event there was such a violation, consistent with its statutory and delegated authority;

(G) prepare a classified ex parte record of review, which shall consist of the appropriate documentation of its review of the qualifying complaint and the classified decision described in subsection (c)(i)(F) of this section; and

(H) provide any necessary support to the Data Protection Review Court.

(ii) Binding effect. Each element of the Intelligence Community, and each agency containing an element of the Intelligence Community, shall comply with any determination by the CLPO to undertake appropriate remediation pursuant to subsection (c)(i)(C) of this section, subject to any contrary determination by the Data Protection Review Court.

(iii) Assistance. Each element of the Intelligence Community shall provide the CLPO with access to information necessary to conduct the reviews described in subsection (c)(i) of this section, consistent with the protection of intelligence sources and methods, and shall not take any actions designed to impede or improperly influence the CLPO’s reviews. Privacy and civil liberties officials within elements of the Intelligence Community shall also support the CLPO as it performs the reviews described in subsection (c)(i) of this section.

(iv) Independence. The Director shall not interfere with a review by the CLPO of a qualifying complaint under subsection (c)(i) of this section; nor shall the Director remove the CLPO for any actions taken pursuant to

**EXECUTIVE ORDER 14086: ENHANCING SAFEGUARDS FOR UNITED STATES
SIGNALS INTELLIGENCE ACTIVITIES**

this order, except for instances of misconduct, malfeasance, breach of security, neglect of duty, or incapacity.

(d) Data Protection Review Court.

(i) Establishment. The Attorney General is authorized to and shall establish a process to review determinations made by the CLPO under subsection (c)(i) of this section. In exercising that authority, the Attorney General shall, within 60 days of the date of this order, promulgate regulations establishing a Data Protection Review Court to exercise the Attorney General's authority to review such determinations. These regulations shall, at a minimum, provide that:

(A) The Attorney General, in consultation with the Secretary of Commerce, the Director, and the PCLOB, shall appoint individuals to serve as judges on the Data Protection Review Court, who shall be legal practitioners with appropriate experience in the fields of data privacy and national security law, giving weight to individuals with prior judicial experience, and who shall not be, at the time of their initial appointment, employees of the United States Government.

During their term of appointment on the Data Protection Review Court, such judges shall not have any official duties or employment within the United States Government other than their official duties and employment as judges on the Data Protection Review Court.

(B) Upon receipt of an application for review filed by the complainant or an element of the Intelligence Community of a determination made by the CLPO under subsection (c) of this section, a three-judge panel of the Data Protection Review Court shall be convened to review the application. Service on the Data Protection Review Court panel shall require that the judge hold the requisite security clearances to access classified national security information.

(C) Upon being convened, the Data Protection Review Court panel shall select a special advocate through procedures prescribed in the Attorney General's regulations. The special advocate shall assist the panel in its consideration of the application for review, including by advocating regarding the complainant's interest in the matter and ensuring that the Data Protection Review Court panel is well informed of the issues and the law with respect to the matter. Service as a special advocate shall require that the special advocate hold the requisite security clearances to access classified national security information and to adhere to restrictions prescribed in the Attorney General's regulations on communications with the complainant to ensure the

**EXECUTIVE ORDER 14086: ENHANCING SAFEGUARDS FOR UNITED STATES
SIGNALS INTELLIGENCE ACTIVITIES**

protection of classified or otherwise privileged or protected information.

(D) The Data Protection Review Court panel shall impartially review the determinations made by the CLPO with respect to whether a covered violation occurred and the appropriate remediation in the event there was such a violation. The review shall be based at a minimum on the classified ex parte record of review described in subsection (c)(i)(F) of this section and information or submissions provided by the complainant, the special advocate, or an element of the Intelligence Community. In reviewing determinations made by the CLPO, the Data Protection Review Court panel shall be guided by relevant decisions of the United States Supreme Court in the same way as are courts established under Article III of the United States Constitution, including those decisions regarding appropriate deference to relevant determinations of national security officials.

(E) In the event that the Data Protection Review Court panel disagrees with any of the CLPO's determinations with respect to whether a covered violation occurred or the appropriate remediation in the event there was such a violation, the panel shall issue its own determinations.

(F) The Data Protection Review Court panel shall provide a classified report on information indicating a violation of any authority subject to the oversight of the FISC to the Assistant Attorney General for National Security, who shall report violations to the FISC in accordance with its rules of procedure.

(G) After the review is completed, the CLPO shall be informed of the Data Protection Review Court panel's determinations through procedures prescribed by the Attorney General's regulations.

(H) After a review is completed in response to a complainant's application for review, the Data Protection Review Court, through procedures prescribed by the Attorney General's regulations, shall inform the complainant, through the appropriate public authority in a qualifying state and without confirming or denying that the complainant was subject to United States signals intelligence activities, that "the review either did not identify any covered violations or the Data Protection Review Court issued a determination requiring appropriate remediation."

(ii) Binding effect. Each element of the Intelligence Community, and each agency containing an element of the Intelligence Community, shall comply with any determination by a Data Protection Review Court panel to undertake appropriate remediation.

EXECUTIVE ORDER 14086: ENHANCING SAFEGUARDS FOR UNITED STATES SIGNALS INTELLIGENCE ACTIVITIES

(iii) Assistance. Each element of the Intelligence Community shall provide the CLPO with access to information necessary to conduct the review described in subsection (d)(i) of this section, consistent with the protection of intelligence sources and methods, that a Data Protection Review Court panel requests from the CLPO and shall not take any actions for the purpose of impeding or improperly influencing a panel's review.

(iv) Independence. The Attorney General shall not interfere with a review by a Data Protection Review Court panel of a determination the CLPO made regarding a qualifying complaint under subsection (c)(i) of this section; nor shall the Attorney General remove any judges appointed as provided in subsection (d)(i)(A) of this section, or remove any judge from service on a Data Protection Review Court panel, except for instances of misconduct, malfeasance, breach of security, neglect of duty, or incapacity, after taking due account of the standards in the Rules for Judicial-Conduct and Judicial-Disability Proceedings promulgated by the Judicial Conference of the United States pursuant to the Judicial Conduct and Disability Act (28 U.S.C. 351 et seq.).

(v) Record of determinations. For each qualifying complaint transmitted by the appropriate public authority in a qualifying state, the Secretary of Commerce shall:

(A) maintain a record of the complainant who submitted such complaint;

(B) not later than 5 years after the date of this order and no less than every 5 years thereafter, contact the relevant element or elements of the Intelligence Community regarding whether information pertaining to the review of such complaint by the CLPO has been declassified and whether information pertaining to the review of any application for review submitted to the Data Protection Review Court has been declassified, including whether an element of the Intelligence Community filed an application for review with the Data Protection Review Court; and

(C) if informed that such information has been declassified, notify the complainant, through the appropriate public authority in a qualifying state, that information pertaining to the review of their complaint by the CLPO or to the review of any application for review submitted to the Data Protection Review Court may be available under applicable law.

(e) Annual review by PCLOB of redress process.

**EXECUTIVE ORDER 14086: ENHANCING SAFEGUARDS FOR UNITED STATES
SIGNALS INTELLIGENCE ACTIVITIES**

- (i) Nature of review. Consistent with applicable law, the PCLOB is encouraged to conduct an annual review of the processing of qualifying complaints by the redress mechanism established by section 3 of this order, including whether the CLPO and the Data Protection Review Court processed qualifying complaints in a timely manner; whether the CLPO and the Data Protection Review Court are obtaining full access to necessary information; whether the CLPO and the Data Protection Review Court are operating consistent with this order; whether the safeguards established by section 2 of this order are properly considered in the processes of the CLPO and the Data Protection Review Court; and whether the elements of the Intelligence Community have fully complied with determinations made by the CLPO and the Data Protection Review Court.
- (ii) Assistance. The Attorney General, the CLPO, and the elements of the Intelligence Community shall provide the PCLOB with access to information necessary to conduct the review described in subsection (e)(i) of this section, consistent with the protection of intelligence sources and methods.
- (iii) Report and certification. Within 30 days of completing any review described in subsection (e)(i) of this section, the PCLOB is encouraged to:
- (A) provide the President, the Attorney General, the Director, the heads of elements of the Intelligence Community, the CLPO, and the congressional intelligence committees with a classified report detailing the results of its review;
 - (B) release to the public an unclassified version of the report; and
 - (C) make an annual public certification as to whether the redress mechanism established pursuant to section 3 of this order is processing complaints consistent with this order.
- (iv) Consideration of review. Within 180 days of receipt of any report by the PCLOB described in subsection (e)(iii)(A) of this section, the Attorney General, the Director, the heads of elements of the Intelligence Community, and the CLPO shall carefully consider and shall implement or otherwise address all recommendations contained in such report, consistent with applicable law.
- (f) Designation of qualifying state.
- (i) To implement the redress mechanism established by section 3 of this order, the Attorney General is authorized to designate a country or regional economic integration organization as a qualifying state for purposes of the redress mechanism established pursuant to section 3 of this order, effective immediately or on a date specified by the Attorney

EXECUTIVE ORDER 14086: ENHANCING SAFEGUARDS FOR UNITED STATES SIGNALS INTELLIGENCE ACTIVITIES

General, if the Attorney General determines, in consultation with the Secretary of State, the Secretary of Commerce, and the Director, that:

- (A) the laws of the country, the regional economic integration organization, or the regional economic integration organization's member countries require appropriate safeguards in the conduct of signals intelligence activities for United States persons' personal information that is transferred from the United States to the territory of the country or a member country of the regional economic integration organization;
- (B) the country, the regional economic integration organization, or the regional economic integration organization's member countries of the regional economic integration organization permit, or are anticipated to permit, the transfer of personal information for commercial purposes between the territory of that country or those member countries and the territory of the United States; and
- (C) such designation would advance the national interests of the United States.

(ii) The Attorney General may revoke or amend such a designation, effective immediately or on a date specified by the Attorney General, if the Attorney General determines, in consultation with the Secretary of State, the Secretary of Commerce, and the Director, that:

- (A) the country, the regional economic integration organization, or the regional economic integration organization's member countries do not provide appropriate safeguards in the conduct of signals intelligence activities for United States persons' personal information that is transferred from the United States to the territory of the country or to a member country of the regional economic integration organization;
- (B) the country, the regional economic integration organization, or the regional economic integration organization's member countries do not permit the transfer of personal information for commercial purposes between the territory of that country or those member countries and the territory of the United States; or
- (C) such designation is not in the national interests of the United States.

Sec. 4. Definitions. For purposes of this order:

- (a) "Appropriate remediation" means lawful measures designed to fully redress an identified covered violation regarding a specific complainant and limited to measures designed to address that specific complainant's complaint, taking into account the ways that a violation of the kind identified

EXECUTIVE ORDER 14086: ENHANCING SAFEGUARDS FOR UNITED STATES SIGNALS INTELLIGENCE ACTIVITIES

have customarily been addressed. Such measures may include, depending on the specific covered violation at issue, curing through administrative measures violations found to have been procedural or technical errors relating to otherwise lawful access to or handling of data, terminating acquisition of data where collection is not lawfully authorized, deleting data that had been acquired without lawful authorization, deleting the results of inappropriately conducted queries of otherwise lawfully collected data, restricting access to lawfully collected data to those appropriately trained, or recalling intelligence reports containing data acquired without lawful authorization or that were otherwise disseminated in a manner inconsistent with United States law. Appropriate remediation shall be narrowly tailored to redress the covered violation and to minimize adverse impacts on the operations of the Intelligence Community and the national security of the United States.

(b) “Bulk collection” means the authorized collection of large quantities of signals intelligence data that, due to technical or operational considerations, is acquired without the use of discriminants (for example, without the use of specific identifiers or selection terms).

(c) “Counterintelligence” shall have the same meaning as it has in Executive Order 12333.

(d) “Covered violation” means a violation that:

(i) arises from signals intelligence activities conducted after the date of this order regarding data transferred to the United States from a qualifying state after the effective date of the Attorney General’s designation for such state, as provided in section 3(f)(i) of this order;

(ii) adversely affects the complainant’s individual privacy and civil liberties interests; and

(iii) violates one or more of the following:

(A) the United States Constitution;

(B) the applicable sections of FISA or any applicable FISC-approved procedures;

(C) Executive Order 12333 or any applicable agency procedures pursuant to Executive Order 12333;

(D) this order or any applicable agency policies and procedures issued or updated pursuant to this order (or the policies and procedures identified in section 2(c)(iv)(A) of this order before they are updated pursuant to section 2(c)(iv)(B) of this order);

(E) any successor statute, order, policies, or procedures to those identified in section 4(d)(iii)(B)–(D) of this order; or

EXECUTIVE ORDER 14086: ENHANCING SAFEGUARDS FOR UNITED STATES SIGNALS INTELLIGENCE ACTIVITIES

(F) any other statute, order, policies, or procedures adopted after the date of this order that provides privacy and civil liberties safeguards with respect to United States signals intelligence activities within the scope of this order, as identified in a list published and updated by the Attorney General, in consultation with the Director of National Intelligence.

(e) “Foreign intelligence” shall have the same meaning as it has in Executive Order 12333.

(f) “Intelligence” shall have the same meaning as it has in Executive Order 12333.

(g) “Intelligence Community” and “elements of the Intelligence Community” shall have the same meaning as they have in Executive Order 12333.

(h) “National security” shall have the same meaning as it has in Executive Order 13526 of December 29, 2009 (Classified National Security Information).

(i) “Non-United States person” means a person who is not a United States person.

(j) “Personnel of the United States or of its allies or partners” means any current or former member of the Armed Forces of the United States, any current or former official of the United States Government, and any other person currently or formerly employed by or working on behalf of the United States Government, as well as any current or former member of the military, current or former official, or other person currently or formerly employed by or working on behalf of an ally or partner.

(k) “Qualifying complaint” means a complaint, submitted in writing, that:

(i) alleges a covered violation has occurred that pertains to personal information of or about the complainant, a natural person, reasonably believed to have been transferred to the United States from a qualifying state after the effective date of the Attorney General’s designation for such state, as provided in section 3(f)(i) of this order;

(ii) includes the following basic information to enable a review: information that forms the basis for alleging that a covered violation has occurred, which need not demonstrate that the complainant’s data has in fact been subject to United States signals intelligence activities; the nature of the relief sought; the specific means by which personal information of or about the complainant was believed to have been transmitted to the United States; the identities of the United States Government entities believed to be involved in the alleged violation (if

EXECUTIVE ORDER 14086: ENHANCING SAFEGUARDS FOR UNITED STATES SIGNALS INTELLIGENCE ACTIVITIES

known); and any other measures the complainant pursued to obtain the relief requested and the response received through those other measures;

(iii) is not frivolous, vexatious, or made in bad faith;

(iv) is brought on behalf of the complainant, acting on that person's own behalf, and not as a representative of a governmental, nongovernmental, or intergovernmental organization; and

(v) is transmitted by the appropriate public authority in a qualifying state, after it has verified the identity of the complainant and that the complaint satisfies the conditions of section 5(k)(i)–(iv) of this order.

(l) “Significant incident of non-compliance” shall mean a systemic or intentional failure to comply with a principle, policy, or procedure of applicable United States law that could impugn the reputation or integrity of an element of the Intelligence Community or otherwise call into question the propriety of an Intelligence Community activity, including in light of any significant impact on the privacy and civil liberties interests of the person or persons concerned.

(m) “United States person” shall have the same meaning as it has in Executive Order 12333.

(n) “Validated intelligence priority” shall mean, for most United States signals intelligence collection activities, a priority validated under the process described in section 2(b)(iii) of this order; or, in narrow circumstances (for example, when such process cannot be carried out because of a need to address a new or evolving intelligence requirement), shall mean a priority set by the President or the head of an element of the Intelligence Community in accordance with the criteria described in section 2(b)(iii)(A)(1)–(3) of this order to the extent feasible.

(o) “Weapons of mass destruction” shall have the same meaning as it has in Executive Order 13526.

Sec. 5. General Provisions.

(a) Nothing in this order shall be construed to impair or otherwise affect:

(i) the authority granted by law to an executive department, agency, or the head thereof; or

(ii) the functions of the Director of the Office of Management and Budget relating to budgetary, administrative, or legislative proposals.

(b) This order shall be implemented consistent with applicable law, including orders of and procedures approved by the FISC, and subject to the availability of appropriations.

(c) Nothing in this order precludes the application of more privacy-protective safeguards for United States signals intelligence activities that would apply

EXECUTIVE ORDER 14086: ENHANCING SAFEGUARDS FOR UNITED STATES SIGNALS INTELLIGENCE ACTIVITIES

in the absence of this order. In the case of any conflict between this order and other applicable law, the more privacy-protective safeguards shall govern the conduct of signals intelligence activities, to the maximum extent allowed by law.

(d) Nothing in this order prohibits elements of the Intelligence Community from disseminating information relating to a crime for law enforcement purposes; disseminating warnings of threats of killing, serious bodily injury, or kidnapping; disseminating cyber threat, incident, or intrusion response information; notifying victims or warning potential victims of crime; or complying with dissemination obligations required by statute, treaty, or court order, including orders of and procedures approved by the FISC or other court orders.

(e) The collection, retention, and dissemination of information concerning United States persons is governed by multiple legal and policy requirements, such as those required by FISA and Executive Order 12333. This order is not intended to alter the rules applicable to United States persons adopted pursuant to FISA, Executive Order 12333, or other applicable law.

(f) This order shall apply to signals intelligence activities consistent with the scope of PPD–28’s application to such activities prior to PPD–28’s partial revocation by the national security memorandum issued concurrently with this order. To implement this subsection, the head of each agency containing an element of the Intelligence Community, in consultation with the Attorney General and the Director, is hereby delegated the authority to issue guidance, which may be classified, as appropriate, as to the scope of application of this order with respect to the element or elements of the Intelligence Community within their agency. The CLPO and the Data Protection Review Court, in carrying out the functions assigned to it under this order, shall treat such guidance as authoritative and binding.

(g) Nothing in this order confers authority to declassify or disclose classified national security information except as authorized pursuant to Executive Order 13526 or any successor order. Consistent with the requirements of Executive Order 13526, the CLPO, the Data Protection Review Court, and the special advocates shall not have authority to declassify classified national security information, nor shall they disclose any classified or otherwise privileged or protected information except to authorized and appropriately cleared individuals who have a need to know the information.

(h) This order creates an entitlement to submit qualifying complaints to the CLPO and to obtain review of the CLPO’s decisions by the Data Protection Review Court in accordance with the redress mechanism established in section 3 of this order. This order is not intended to, and does not, create any

**EXECUTIVE ORDER 14086: ENHANCING SAFEGUARDS FOR UNITED STATES
SIGNALS INTELLIGENCE ACTIVITIES**

other entitlement, right, or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person. This order is not intended to, and does not, modify the availability or scope of any judicial review of the decisions rendered through the redress mechanism, which is governed by existing law.

THE WHITE HOUSE,
October 7, 2022.

**NATIONAL SECURITY MEMORANDUM ON PARTIAL REVOCATION
OF PRESIDENTIAL POLICY DIRECTIVE 28**

October 7, 2022

NATIONAL SECURITY MEMORANDUM/NSM-14

SUBJECT: Partial Revocation of Presidential Policy Directive 28

The Executive Order of October 7, 2022 (Enhancing Safeguards for United States Signals Intelligence Activities), establishes enhanced safeguards for United States signals intelligence activities that supersede the safeguards for personal information collected through signals intelligence established by Presidential Policy Directive 28 of January 17, 2014 (Signals Intelligence Activities) (PPD-28). The Executive Order establishes enhanced safeguards in recognition that signals intelligence activities must be conducted in a manner that takes into account that all persons should be treated with dignity and respect, regardless of their nationality or wherever they might reside, and that all persons have legitimate privacy interests in the handling of their personal information. In addition, signals intelligence activities present the potential for national security damage if improperly disclosed. Therefore, it is essential to maintain the policy process refined by section 3 of PPD-28 and supplemented by the classified annex to PPD-28, under which national security policymakers consider carefully the value of signals intelligence activities to our national interests and the risks entailed in conducting those activities.

Section 1. Revocation. PPD-28 is hereby revoked except for sections 3 and 6 of that directive and the classified annex to that directive, which remain in effect.

Section 2. General Provisions. (a) Nothing in this memorandum shall be construed to impair or otherwise affect:

- (i) the authority granted by law to an executive department, agency, or the head thereof; or
- (ii) the functions of the Director of the Office of Management and Budget relating to budgetary, administrative, or legislative proposals.

PRESIDENTIAL POLICY DIRECTIVE 28

(b) This memorandum shall be implemented consistent with applicable law and subject to the availability of appropriations.

(c) This memorandum is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

JOSEPH R. BIDEN JR.

**PRESIDENTIAL POLICY DIRECTIVE – SIGNALS INTELLIGENCE
ACTIVITIES**

January 17, 2014

PRESIDENTIAL POLICY DIRECTIVE/PPD-28

SUBJECT: Signals Intelligence Activities

The United States, like other nations, has gathered intelligence throughout its history to ensure that national security and foreign policy decision makers have access to timely, accurate, and insightful information.

The collection of signals intelligence is necessary for the United States to advance its national security and foreign policy interests and to protect its citizens and the citizens of its allies and partners from harm. At the same time, signals intelligence activities and the possibility that such activities may be improperly disclosed to the public pose multiple risks. These include risks to: our relationships with other nations, including the cooperation we receive from other nations on law enforcement, counterterrorism, and other issues; our commercial, economic, and financial interests, including a potential loss of international trust in U.S. firms and the decreased willingness of other nations to participate in international data sharing, privacy, and regulatory regimes; the credibility of our commitment to an open, interoperable, and secure global Internet; and the protection of intelligence sources and methods.

In addition, our signals intelligence activities must take into account that all persons should be treated with dignity and respect, regardless of their nationality or wherever they might reside, and that all persons have legitimate privacy interests in the handling of their personal information.

In determining why, whether, when, and how the United States conducts signals intelligence activities, we must weigh all of these considerations in a context in which information and communications technologies are constantly changing. The evolution of technology has created a world where communications important to our national security and the communications all of us make as part of our daily lives are transmitted through the same channels. This presents new and diverse opportunities for, and challenges with respect to, the collection of intelligence – and especially signals intelligence. The United States Intelligence Community (IC) has achieved remarkable success in developing enhanced capabilities to perform its signals intelligence mission in this rapidly changing

world, and these enhanced capabilities are a major reason we have been able to adapt to a dynamic and challenging security environment.¹ The United States must preserve and continue to develop a robust and technologically advanced signals intelligence capability to protect our security and that of our partners and allies. Our signals intelligence capabilities must also be agile enough to enable us to focus on fleeting opportunities or emerging crises and to address not only the issues of today, but also the issues of tomorrow, which we may not be able to foresee.

Advanced technologies can increase risks, as well as opportunities, however, and we must consider these risks when deploying our signals intelligence capabilities. The IC conducts signals intelligence activities with care and precision to ensure that its collection, retention, use, and dissemination of signals intelligence account for these risks. In light of the evolving technological and geopolitical environment, we must continue to ensure that our signals intelligence policies and practices appropriately take into account our alliances and other partnerships; the leadership role that the United States plays in upholding democratic principles and universal human rights; the increased globalization of trade, investment, and information flows; our commitment to an open, interoperable and secure global Internet; and the legitimate privacy and civil liberties concerns of U.S. citizens and citizens of other nations.

Presidents have long directed the acquisition of foreign intelligence and counterintelligence² pursuant to their constitutional authority to conduct U.S. foreign relations and to fulfill their constitutional responsibilities as Commander in Chief and Chief Executive. They have also provided direction on the conduct of intelligence activities in furtherance of these authorities and responsibilities, as well as in execution of laws enacted by the Congress. Consistent with this historical practice, this directive articulates principles to guide why, whether,

¹ For the purposes of this directive, the terms “Intelligence Community” and “elements of the Intelligence Community” shall have the same meaning as they do in Executive Order 12333 of December 4, 1981, as amended (Executive Order 12333).

² For the purposes of this directive, the terms “foreign intelligence” and “counterintelligence” shall have the same meaning as they have in Executive Order 12333. Thus, “foreign intelligence” means “information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, foreign persons, or international terrorists,” and “counterintelligence” means “information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, or persons, or their agents, or international terrorist organizations or activities.” Executive Order 12333 further notes that “[i]ntelligence includes foreign intelligence and counterintelligence.”

PRESIDENTIAL POLICY DIRECTIVE 28

when, and how the United States conducts signals intelligence activities for authorized foreign intelligence and counterintelligence purposes.³

SEC. 3. REFINING THE PROCESS FOR COLLECTING SIGNALS INTELLIGENCE.

U.S. intelligence collection activities present the potential for national security damage if improperly disclosed. Signals intelligence collection raises special concerns, given the opportunities and risks created by the constantly evolving technological and geopolitical environment; the unique nature of such collection and the inherent concerns raised when signals intelligence can only be collected in bulk; and the risk of damage to our national security interests and our law enforcement, intelligence-sharing, and diplomatic relationships should our capabilities or activities be compromised. It is, therefore, essential that national security policymakers consider carefully the value of signals intelligence activities in light of the risks entailed in conducting these activities.

To enable this judgment, the heads of departments and agencies that participate in the policy processes for establishing signals intelligence priorities and requirements shall, on an annual basis, review any priorities or requirements identified by their departments or agencies and advise the DNI whether each should be maintained, with a copy of the advice provided to the APNSA.

Additionally, the classified Annex to this directive, which supplements the existing policy process for reviewing signals intelligence activities, affirms that determinations about whether and how to conduct signals intelligence activities must carefully evaluate the benefits to our national interests and the risks posed by those activities.⁴

SEC. 6. GENERAL PROVISIONS.

(a) Nothing in this directive shall be construed to prevent me from exercising my constitutional authority, including as Commander in Chief, Chief Executive, and in the conduct of foreign affairs, as well as my statutory authority. Consistent

³ Unless otherwise specified, this directive shall apply to signals intelligence activities conducted in order to collect communications or information about communications, except that it shall not apply to signals intelligence activities undertaken to test or develop signals intelligence capabilities.

⁴ Section 3 of this directive, and the directive's classified Annex, do not apply to (1) signals intelligence activities undertaken by or for the Federal Bureau of Investigation in support of predicated investigations other than those conducted solely for purposes of acquiring foreign intelligence; or (2) signals intelligence activities undertaken in support of military operations in an area of active hostilities, covert action, or human intelligence operations.

PRESIDENTIAL POLICY DIRECTIVE 28

with this principle, a recipient of this directive may at any time recommend to me, through the APNSA, a change to the policies and procedures contained in this directive.

(b) Nothing in this directive shall be construed to impair or otherwise affect the authority or responsibility granted by law to a United States Government department or agency, or the head thereof, or the functions of the Director of OMB relating to budgetary, administrative, or legislative proposals. This directive is intended to supplement existing processes or procedures for reviewing foreign intelligence or counterintelligence activities and should not be read to supersede such processes and procedures unless explicitly stated.

(c) This directive shall be implemented consistent with applicable U.S. law and subject to the availability of appropriations.

(d) This directive is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

**PRESIDENTIAL POLICY DIRECTIVE – PROTECTING
WHISTLEBLOWERS WITH ACCESS TO CLASSIFIED INFORMATION**

October 10, 2012

PRESIDENTIAL POLICY DIRECTIVE/PPD-19

SUBJECT: Protecting Whistleblowers with Access to Classified Information

This Presidential Policy Directive ensures that employees (1) serving in the Intelligence Community or (2) who are eligible for access to classified information can effectively report waste, fraud, and abuse while protecting classified national security information. It prohibits retaliation against employees for reporting waste, fraud, and abuse.

To ensure the timely and effective implementation of the goals of this directive, I hereby direct that the following actions be taken:

A. Prohibition on Retaliation in the Intelligence Community

Any officer or employee of a Covered Agency who has authority to take, direct others to take, recommend, or approve any Personnel Action, shall not, with respect to such authority, take or fail to take, or threaten to take or fail to take, a Personnel Action with respect to any employee serving in an Intelligence Community Element as a reprisal for a Protected Disclosure.

Within 270 days of the date of this directive, the head of each Intelligence Community Element shall certify to the Director of National Intelligence (DNI) that the personnel policies that apply to that element provide a process for employees to seek review of Personnel Actions they allege to be in violation of this directive and that the review process is consistent with the requirements of this directive. Such review process shall apply to Personnel Actions that arise after the date on which the department or agency (“agency”) head certifies the agency review process. If the head of any Intelligence Community Element fails to make this certification or if the DNI disagrees with the certification, the DNI shall notify the President.

The review process required by the above paragraph shall be consistent, to the fullest extent possible, with the policies and procedures used to adjudicate alleged violations of section 2302(b)(8) of title 5, United States Code. The review process shall provide for the protection of classified national security information

and intelligence sources and methods. As part of the review process, the agency Inspector General shall conduct a review to determine whether a Personnel Action violated this directive and may recommend that the agency take specific corrective action to return the employee, as nearly as practicable and reasonable, to the position such employee would have held had the reprisal not occurred. An agency head shall carefully consider the findings of and actions recommended by the agency Inspector General. To the extent authorized by law (including the Back Pay Act), corrective action may include, but is not limited to, reinstatement, reassignment, the award of reasonable attorney's fees, other reasonable costs, back pay and related benefits, travel expenses, and compensatory damages.

B. Prohibition on Retaliation by Affecting Eligibility for Access to Classified Information

Any officer or employee of an executive branch agency who has authority to take, direct others to take, recommend, or approve any action affecting an employee's Eligibility for Access to Classified Information shall not, with respect to such authority, take or fail to take, or threaten to take or fail to take, any action affecting an employee's Eligibility for Access to Classified Information as a reprisal for a Protected Disclosure.

Within 270 days of the date of this directive, the head of each agency in possession of classified information shall certify to the DNI, acting in his or her capacity as the head of the entity selected by the President under subsection 435b(b) of title 50, United States Code, and as the Security Executive Agent designated in Executive Order 13467 of June 30, 2008, that the agency has a review process that permits employees to appeal actions affecting Eligibility for Access to Classified Information they allege to be in violation of this directive and that the review process is consistent with the requirements of this directive. Such review process shall apply to actions that arise after the date on which the agency head certifies the agency review process. If the head of any agency fails to make this certification or if the DNI disagrees with the certification, the DNI shall notify the President.

The review process required by the above paragraph shall, to the fullest extent possible, be consistent with and integrated into the policies and procedures used to review security clearance determinations under Section 5.2 of Executive Order 12968 of August 2, 1995, as amended. The review process shall provide for the protection of classified national security information and intelligence sources and methods. As part of the review process, the agency Inspector General shall conduct a review to determine whether an action affecting Eligibility for Access

PRESIDENTIAL POLICY DIRECTIVE 19

to Classified Information violated this directive and may recommend that the agency reconsider the employee's Eligibility for Access to Classified Information consistent with the national security and with Executive Order 12968 and recommend that the agency take other corrective action to return the employee, as nearly as practicable and reasonable, to the position such employee would have held had the reprisal not occurred. An agency head shall carefully consider the findings of and actions recommended by the agency Inspector General. To the extent authorized by law (including the Back Pay Act), corrective action may include, but is not limited to, reinstatement, reassignment, reasonable attorney's fees, other reasonable costs, back pay and related benefits, travel expenses, and compensatory damages.

C. Inspector General External Review Panel

An employee alleging a reprisal who has exhausted the applicable review process required by Section A or B of this directive may request an external review by a three-member Inspector General panel (External Review Panel) chaired by the Inspector General of the Intelligence Community (on behalf of the DNI, acting in his capacity as the head of the entity selected by the President under subsection 435b(b) of title 50, United States Code, and as the Security Executive Agent designated in Executive Order 13467 of June 30, 2008). If such a request is made, the Inspector General of the Intelligence Community shall decide, in his or her discretion, whether to convene the External Review Panel, and, if so, shall designate two other panel members from the Inspectors General of the following agencies: Departments of State, the Treasury, Defense, Justice, Energy, and Homeland Security and Central Intelligence Agency. The Inspector General from the agency that completed the initial review shall not be a member of the External Review Panel. The External Review Panel shall complete a review of the claim, which may consist of a file review, as appropriate, within 180 days.

If the External Review Panel determines that the individual was the subject of a Personnel Action prohibited by Section A while an employee of a Covered Agency or an action affecting his or her Eligibility for Access to Classified Information prohibited by Section B, the panel may recommend that the agency head take corrective action to return the employee, as nearly as practicable and reasonable, to the position such employee would have held had the reprisal not occurred and that the agency head reconsider the employee's Eligibility for Access to Classified Information consistent with the national security and with Executive Order 12968.

PRESIDENTIAL POLICY DIRECTIVE 19

An agency head shall carefully consider the recommendation of the External Review Panel pursuant to the above paragraph and within 90 days, inform the panel and the DNI of what action he or she has taken. If the head of any agency fails to so inform the DNI, the DNI shall notify the President.

On an annual basis, the Inspector General of the Intelligence Community shall report the determinations and recommendations and department and agency head responses to the DNI and, as appropriate, to the relevant congressional committees.

With respect to matters covered by this directive, all agencies shall cooperate with their respective agency Inspectors General, the Inspector General of the Intelligence Community, and External Review Panels and provide such information and assistance to their respective agency Inspectors General, the Inspector General of the Intelligence Community, and members of External Review Panels as such Inspectors General may request, to the extent permitted by law.

D. Policies and Procedures

Within 365 days of the date of this directive, the DNI shall, in consultation with the Secretary of Defense, the Attorney General, and the heads of agencies containing Intelligence Community Elements, issue policies and procedures for ensuring that all employees serving in Intelligence Community Elements are aware of the protections and review processes available to individuals who make Protected Disclosures. These policies and procedures shall to the extent practicable be publically available, and shall provide:

- (1) guidance for individual officers or employees regarding what disclosures are protected;
- (2) guidance for potential recipients on the appropriate handling of Protected Disclosures, including for referral by the DNI or Inspector General of the Intelligence Community to appropriate agency officials of any Protected Disclosures unrelated to national intelligence; and
- (3) information regarding the review processes required by Sections A, B, and C of this directive.

E. Review of Regulations Implementing Section 2303 of Title 5, United States Code

Within 180 days of the date of this directive, the Attorney General, in consultation with the Special Counsel and Federal Bureau of Investigation employees, shall deliver a report to the President that assesses the efficacy of the provisions contained in part 27 of title 28, Code of Federal Regulations in deterring the personnel practices prohibited in section 2303 of title 5, United States Code, and ensuring appropriate enforcement of that section, and describes any proposed revisions to the provisions contained in Part 27 of title 28 that would increase their effectiveness in fulfilling the purposes of section 2303 of title 5, United States Code.

F. Definitions

For purposes of this directive:

(1) The term “Covered Agency” means an executive department or independent establishment, as defined under sections 101 and 104 of title 5, United States Code, that contains or constitutes an Intelligence Community Element, as defined below.

(2) The term “Eligibility for Access to Classified Information” means the result of the determination whether an employee (a) is eligible for access to classified information in accordance with Executive Order 12968 (relating to access to classified information), or any successor thereto, and Executive Order 10865 of February 20, 1960, as amended (relating to safeguarding classified information with industry), or any successor thereto; and (b) possesses a need to know under such orders.

(3) The term “Intelligence Community Element” means any executive agency or unit thereof determined by the President under section 2302(a)(2)(C)(ii) of title 5, United States Code, to have as its principal function the conduct of foreign intelligence or counterintelligence activities, including but not limited to the Office of the DNI, the Central Intelligence Agency, the National Security Agency, the Defense Intelligence Agency, the National Geospatial-Intelligence Agency, and the National Reconnaissance Office. For purposes of this directive, the term “Intelligence Community Element” does not include the Federal Bureau of Investigation.

(4) The term “Personnel Action” means an appointment, promotion, detail, transfer, reassignment, demotion, suspension, termination,

PRESIDENTIAL POLICY DIRECTIVE 19

reinstatement, restoration, reemployment, or performance evaluation; a decision concerning pay, benefits, or awards; a decision concerning education or training if the education or training may reasonably be expected to lead to an appointment, reassignment, promotion, or performance evaluation; a decision to order psychiatric testing or examination; and any other significant change in duties, responsibilities, or working conditions.

The term “Personnel Action” does not include the termination of an employee pursuant to section 1609 of title 10, United States Code. The term “Personnel Action” does not include the termination of an employee pursuant to section 102A(m) of the National Security Act of 1947, section 104A(e) of the National Security Act of 1947, or section 7532 of title 5, United States Code, so long as the official authorized by those provisions to terminate the employee (and not his or her delegee) (i) determines that the alternative legal procedures to terminate the employee cannot be invoked in a manner consistent with the national security and (ii) promptly notifies the Inspector General of the employing agency. The term “Personnel Action” does not include actions taken with respect to a position that the agency head has designated, prior to the action as being of a confidential, policy determining, policymaking, or policy advocating character. The term “Personnel Action” does not include actions taken with respect to a member of the Armed Forces, as used in section 1034 of Title 10, United States Code. The term “Personnel Action” does not include any actions taken prior to the issuance of this directive.

(5) The term “Protected Disclosure” means:

(a) a disclosure of information by the employee to a supervisor in the employee’s direct chain of command up to and including the head of the employing agency, to the Inspector General of the employing agency or Intelligence Community Element, to the Director of National Intelligence, to the Inspector General of the Intelligence Community, or to an employee designated by any of the above officials for the purpose of receiving such disclosures, that the employee reasonably believes evidences (i) a violation of any law, rule, or regulation; or (ii) gross mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety;

(b) any communication described by and that complies with subsection (a)(1), (d), or (h) of section 8H of the Inspector General Act of 1978 (5 U.S.C. App.); subsection (d)(5)(A) of section 17 of the Central

PRESIDENTIAL POLICY DIRECTIVE 19

Intelligence Agency Act of 1949 (50 U.S.C. 403q); or subsection (k)(5)(A), (D), or (G), of section 103H of the National Security Act of 1947 (50 U.S.C. 403-3h);

(c) the exercise of any appeal, complaint, or grievance with regard to the violation of Section A or B of this directive;

(d) lawfully participating in an investigation or proceeding regarding a violation of Section A or B of this directive; or

(e) cooperating with or disclosing information to an Inspector General, in accordance with applicable provisions of law in connection with an audit, inspection, or investigation conducted by the Inspector General,

if the actions described under subparagraphs (c) through (e) do not result in the employee disclosing classified information or other information contrary to law.

G. General Provisions This directive shall be implemented in a manner consistent with applicable law, including all statutory authorities of the heads of agencies and Inspectors General, and does not restrict available rights, procedures, and remedies under section 2302(b) of Title 5, United States Code.

This directive is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

BARACK OBAMA

**CRITERIA ON THRESHOLDS FOR REPORTING INTELLIGENCE
OVERSIGHT MATTERS AND INSTRUCTIONS RELATING TO
FORMATTING AND SCHEDULING**

Intelligence oversight reporting serves as an early warning of intelligence activities of which the President should be informed, through either his Intelligence Oversight Board (IOB) or the Director of National Intelligence (DNI), or both, and provides a means by which the Executive Branch may quickly identify and correct in a timely manner any deficiencies in the conduct of its intelligence activities. The following criteria on thresholds for reporting intelligence oversight matters to the IOB, and instructions on formatting and scheduling of reports, are issued under the authority of Executive Order 13462, as amended.

I. CRITERIA ON THRESHOLDS FOR REPORTING. The heads of departments with organizations in the Intelligence Community (IC), or the heads of such organizations, or their designees, shall:

(A) Report to the IOB, with copies to the DNI, any intelligence activity which there is reason to believe may be unlawful or contrary to executive order (EO) or presidential directive (PD). The following guidance applies to determining whether a particular matter should be reported:

- (1) “Intelligence activities” has the meaning specified in Part 3.5(g) of EO 12333 and, for purposes of these criteria, include, but are not limited to, the acquisition, collection, retention, analysis, and dissemination of intelligence information.
- (2) Intelligence activities are reportable if a reasonable person would believe they may be unlawful or contrary to EO or PD without waiting for substantiation, investigation, formal adjudication, or resolution of the issue of whether a particular matter is unlawful or contrary to EO or PD.
- (3) Intelligence activities to be reported under EOs 13462 and 12333 are not limited to those that concern “United States persons,” as defined in Part 3.5(k) of EO 12333 or in any successor EO.
- (4) “Executive order or presidential directive” means, for purposes of implementing these criteria, a document signed by the President of the United States that has the force of law for the Executive Branch or constitutes the exercise by the President of his Executive authority. Violations of procedures and guidelines that heads of

OVERSIGHT REPORTING THRESHOLDS

departments or IC components have established to implement EO 12333, or a successor order, should be reported if such matters are of potential presidential interest or deemed appropriate for the IOB's review, e.g., because they involve the apparent violation of substantive rights of individuals.

(5) Reportable events include the initiation of, and significant developments in, investigations or other inquiries relating to the legality or propriety of intelligence activities.

(6) Initial reports made on the basis of incomplete or inaccurate reporting are to be updated as additional information becomes available. Subsequent or updated reports should be identified in such a manner that they can be accurately related to the relevant initial reports.

(7) Intelligence activities are reportable to the IOB if such activities are required to be reported or have been reported to the Attorney General as required by law or other directive, including the Memorandum of Understanding on Reporting of Information Concerning Federal Crimes (1995).

(8) Any intelligence activity that is to be reported to any congressional committee or member of Congress because it is or may be unlawful or contrary to executive order or otherwise "significant or highly sensitive" (see paragraph B, below) shall also be reported to the IOB and DNI generally before such a congressional report is made. Any report concerning intelligence activities that is submitted to any committee or member of Congress shall also be submitted to the IOB and DNI if the activities were also reportable under these criteria.

(B) Report to the IOB and DNI significant or highly sensitive matters.

(1) "Significant or highly sensitive matters" are intelligence activities (regardless of whether the intelligence activities are unlawful or contrary to executive order or presidential directive), or serious criminal activities by intelligence personnel, that could impugn the reputation or integrity of the IC, or otherwise call into question the propriety of intelligence activities.

(2) Such matters might be manifested by actual or the potential for:

- (a) congressional inquiries or investigations;
- (b) adverse media coverage;
- (c) impact on foreign relations or foreign partners; or
- (d) systemic compromise, loss, or unauthorized disclosure of protected information.

OVERSIGHT REPORTING THRESHOLDS

II. CONTENT OF REPORTS. Intelligence oversight reports should include (to the extent practicable without compromising the timeliness of reporting) the following:

- (A) A narrative describing each intelligence activity in question.
- (B) A statement describing when the matter occurred, when it was discovered and initially reported within the IC element, and if applicable, an explanation for any delay in reporting to the IOB.
- (C) Why the matter is being reported, *i.e.*, it is:
 - (1) a potential violation of law (cite the relevant law, if a judgment has been made);
 - (2) potentially contrary to EO or PD (cite the relevant section or part of the EO or PD);
 - (3) a potential violation of agency procedures (cite the specific rule or procedure, if a judgment has been made);
 - (4) “significant” because . . . ; or
 - (5) “highly sensitive” because . . .
- (D) An explanation and analysis of how or why the incident occurred.
- (E) An assessment of any impact of the incident on national security or international relations, as well as any mitigation efforts, including successes and failures of such efforts.
- (F) Any remedial action the IC element has taken or is taking to prevent recurrence of the incident being reported.
- (G) An assessment of any impact the reported intelligence activity may have on civil liberties or protected privacy rights.
- (H) How the IC element concerned is addressing any information improperly acquired, handled, used, destroyed, etc., as a consequence of the matter being reported.
- (I) Quarterly reports, see section IV.B, shall include a summary of the gravity, frequency, trends, and patterns of matters reported for the quarter.
- (J) Any additional information that the reporting official considers relevant for purposes of fully and completely informing the IOB and the DNI on an intelligence oversight matter.

III. FORMATTING REPORTS. Reports may be formatted in accordance with departmental or agency policies, provided all the substantive information described above is included in each report.

IV. SCHEDULING FOR REPORTING.

- (A) Significant or highly sensitive matters must be reported immediately.
 - (1) Significant or highly sensitive matters may be reported orally, if necessary, and followed up with a written report as soon as possible thereafter. The preference is for written reports.

OVERSIGHT REPORTING THRESHOLDS

(2) Significant or highly sensitive matters, whether or not believed to be unlawful or contrary to EO or PD, shall be reported to the IOB and DNI.

(B) Reports of matters other than significant or highly sensitive matters shall be submitted on a quarterly basis. The first report for the calendar year shall cover 1 January through 31 March, and so on for each quarter of the year.

(C) Quarterly reports are due no later than 60 days following the end of each quarter.

(D) All IC elements must submit reports at least quarterly, even if a component has not been made aware of any reportable matter during the reporting period.

Questions concerning the implementation of EO 13462, or intelligence oversight reporting in general, may be submitted to the IOB's General Counsel, or to the ODNI IOB Team: [ODNI/OIG or ODNI/OGC].

MEMORANDUM OF UNDERSTANDING:
REPORTING OF INFORMATION CONCERNING FEDERAL CRIMES

I. INTRODUCTION

Section 1.7 (a) of Executive Order (E.O.) 12333 requires senior officials of the Intelligence Community to—

report to the Attorney General possible violations of the federal criminal laws by employees and of specified federal criminal laws by any other person as provided in procedures agreed upon by the Attorney General and the head of the department or agency concerned, in a manner consistent with the protection of intelligence sources and methods, as specified in those procedures.

Title 28, United States Code, Section 535 (b) requires that—

[a]ny information, allegation, or complaint received in a department or agency of the executive branch of government relating to violations of title 18 involving Government officers and employees shall be expeditiously reported to the Attorney General by the head of the department or agency, unless—

- (1) the responsibility to perform an investigation with respect thereto is specifically assigned otherwise by another provision of law; or
- (2) as to any department or agency of the Government, the Attorney General directs otherwise with respect to a specified class of information, allegation, or complaint.

This Memorandum of Understanding (MOU) sets forth the procedures by which each agency and organization within the Intelligence Community shall report to the Attorney General and to federal investigative agencies information concerning possible federal crimes by employees of an intelligence agency or organization, or violations of specified federal criminal laws by any other person, which information was collected by it during the performance of its designated intelligence activities, as those activities are defined in E.O. 12333, §§1.8-1.13.

II. DEFINITIONS

(A) “Agency,” as that term is used herein, refers to those agencies and organizations within the Intelligence Community as defined in E.O. 12333, §3.4(f), but excluding the intelligence elements of the Federal Bureau of Investigation and the Department of Treasury.

(B) “Employee,” as that term is used herein, means:

- (1) a staff employee, contract employee, asset, or other person or entity providing service to or acting on behalf of any agency within the intelligence community;

(2) a former officer or employee of any agency within the intelligence community for purposes of an offense committed during such person's employment, and for purposes of an offense involving a violation of 18 U.S.C. § 207 (Conflict of interest); and

(3) any other Government employee on detail to the Agency.

(C) "General Counsel" means the general counsel of the Agency or of the Department of which it is a component or an oversight person designated by such person to act on his/her behalf, and for purposes of these procedures may include an Inspector General or equivalent official if agency or departmental procedures so require or if designated by the agency or department head.

(D) "Inspector General" or "IG" means the inspector general of the Agency or of the department of which the Agency is a component.

(E) "Reasonable basis" exists when there are facts and circumstances, either personally known or of which knowledge is acquired from a source believed to be reasonably trustworthy, that would cause a person of reasonable caution to believe that a crime has been, is being, or will be committed. The question of which federal law enforcement or judicial entity has jurisdiction over the alleged criminal acts shall have no bearing upon the issue of whether a reasonable basis exists.

III. SCOPE

(A) This MOU shall not be construed to authorize or require the Agency, or any person or entity acting on behalf of the Agency, to conduct any investigation not otherwise authorized by law, or to collect any information in a manner not authorized by law.

(B) This MOU ordinarily does not require an intelligence agency or organization to report crimes information that was collected and disseminated to it by another department, agency, or organization. Where, however, the receiving agency is the primary or sole recipient of that information, or if analysis by the receiving agency reveals additional crimes information, the receiving agency shall be responsible for reporting all such crimes information in accordance with the provisions of this MOU.

(C) This MOU does not in any way alter or supersede the obligation of an employee of an intelligence agency to report potential criminal behavior by other employees of that agency to an IG, as required either by statute or by agency regulations, nor affect any protections afforded any persons reporting such behavior to an IG. Nor does this MOU affect any crimes reporting procedures between the IG Offices and the Department of Justice.

(D) This MOU does not in any way alter or supersede any obligation of a department or agency to report to the Attorney General criminal behavior by

MOU: REPORTING OF INFORMATION CONCERNING FEDERAL CRIMES

Government employees not employed by the intelligence community, as required by 28 U.S.C. § 535.

(E) This MOU does not affect the obligation to report to the Federal Bureau of Investigation alleged or suspected espionage activities as required under Section 811(c) of the Intelligence Authorization Act of 1995.

(F) The following crimes information is exempted from the application of this memorandum if the specified conditions are met:

(1) Crimes information that has been reported to an IG;¹

(2) Crimes information received by a Department of Defense intelligence component concerning a Defense intelligence component employee who either is subject to the Uniform Code of Military Justice or is a civilian and has been accused of criminal behavior related to his/her assigned duties or position, if (a) the information is submitted to and investigated by the appropriate Defense Criminal Investigative Organization, and (b) in cases involving crimes committed during the performance of intelligence activities, the General Counsel provides to the Department of Justice a report reflecting the nature of the charges and the disposition thereof;

(3) Information regarding non-employee crimes listed in Section VII that is collected by the intelligence component of a Department also having within it a law enforcement organization where (a) the crime is of the type that the Department's law enforcement organization has jurisdiction to investigate; and (b) the Department's intelligence organization submits that crimes information to the Department's law enforcement organization for investigation and further handling in accordance with Department policies and procedures;²

(4) Crimes information regarding persons who are not employees of the Agency, as those terms are defined in Section II, that involve crimes against property in an amount of \$1,000 or less, or, in the case of Agency employees, crimes against property in an amount of \$500 or less. As to other relatively minor offenses to which this MOU would ordinarily apply, but which, in the General Counsel's opinion, do not warrant reporting pursuant to this MOU, the General Counsel may orally contact

¹ If, however, the IG determines that the reported information is not properly subject to that office's jurisdiction, but that such information may be reportable pursuant to this MOU, the IG may forward the information to the DOJ in compliance with these procedures. Alternatively, the IG may transmit the information to the Agency's General Counsel for a determination of what response, if any, is required by this MOU.

² This MOU does not affect the crimes reporting obligations of any law enforcement and other non-intelligence components of a department, agency, or organization.

MOU: REPORTING OF INFORMATION CONCERNING FEDERAL CRIMES

the Assistant Attorney General, Criminal Division,* or his/her designee. If the Department of Justice concurs with that opinion, no further reporting under these procedures is required. The General Counsel shall maintain an appropriate record of such contacts with the Department. If deemed appropriate by the General Counsel, he/she may take necessary steps to pass such information to the appropriate law enforcement authorities; or

(5) Information, other than that relating to homicide or espionage, regarding crimes that were completed more than ten years prior to the date such allegations became known to the agency. If, however, the Agency has a reasonable basis to believe that the alleged criminal activities occurring ten or more years previously relate to, or are a part of, a pattern of criminal activities that continued within that ten year interval, the reporting procedures herein will apply to those activities.

(G) The Procedures set forth herein are not intended to affect whether an intelligence agency reports to state or local authorities activity that appears to constitute a crime under state law. In the event that an intelligence agency considers it appropriate to report to state or local authorities possible criminal activity that may implicate classified information or intelligence sources or methods, it should inform the AAG, or the designated Deputy AAG, Criminal Division, in accordance with paragraph VIII.C, below; the Criminal Division will consult with the intelligence agency regarding appropriate methods for conveying the information to state or local authorities. In the event that an intelligence agency considers it appropriate to report to state or local authorities possible criminal activity that is not expected to implicate classified information or intelligence sources or methods, it should nevertheless provide a copy of such report to the AAG, or to the designated Deputy AAG, Criminal Division.

IV. GENERAL CONSIDERATIONS: ALLEGATIONS OF CRIMINAL ACTS COMMITTED BY AGENCY EMPLOYEES

(A) This Agreement requires each employee of the Agency to report to the General Counsel or IG facts or circumstances that reasonably indicate to the

* [Pursuant to Attorney General Alberto Gonzales's letter of September 14, 2007, to Director of National Intelligence J. Michael McConnell, within this Memorandum of Understanding all referenced functions of the Assistant Attorney General for the Criminal Division or of the Criminal Division, generally, shall be read to refer to the Assistant Attorney General for National Security and the National Security Division, respectively.]

employee that an employee of an intelligence agency has committed, is committing, or will commit a violation of federal criminal law.³

(B) Except as exempted in Section III, when the General Counsel has received allegations, complaints or information (hereinafter allegations) that an employee of the Agency may have violated, may be violating, or may violate a federal criminal statute, that General Counsel should within a reasonable period of time determine whether there is a reasonable basis to believe that a federal crime has been, is being, or will be committed and that it is a crime which, under this memorandum, must be reported. The General Counsel may, as set forth in Section V, below, conduct a preliminary inquiry for this purpose. If a preliminary inquiry reveals that there is a reasonable basis for the allegations, the General Counsel will follow the reporting procedures set forth in Section VIII, below. If a preliminary inquiry reveals that the allegations are without a reasonable basis, the General Counsel will make a record, as appropriate, of that finding and no reporting under these procedures is required.

V. PRELIMINARY INQUIRY INTO ALLEGATIONS AGAINST AN AGENCY EMPLOYEE

(A) The General Counsel's preliminary inquiry regarding allegations against an Agency employee will ordinarily be limited to the following:

- (1) review of materials submitted in support of the allegations;
- (2) review of Agency indices, records, documents, and files;
- (3) examination of premises occupied by the Agency;
- (4) examination of publicly available federal, state, and local government records and other publicly available records and information;
- (5) interview of the complainant; and
- (6) interview of any Agency employee, other than the accused, who, in the opinion of the General Counsel, may be able to corroborate or refute the allegations.

(B) Where criminal allegations against an Agency employee are subject to this MOU, an interview of that employee may only be undertaken in compliance with the following conditions:

³ When a General Counsel or IG has received information concerning alleged violations of federal law by an employee of another intelligence community agency, and those violations are not exempted under section III. E. 4, hereof, the General Counsel shall notify in writing the General Counsel of the accused employee's agency. The latter General Counsel must then determine whether this MOU requires the allegations to be reported to the Department of Justice.

(1) Where the crime alleged against an Agency employee does not pertain to a serious felony offense,⁴ a responsible Agency official may interview the accused employee; however, such interview shall only be conducted with the approval of the General Counsel, the IG, or, as to Defense and military employees, the responsible military Judge Advocate General or the responsible Defense Criminal Investigative Organization.

(2) Where the crime alleged against an Agency employee is a serious felony offense, the Agency shall ordinarily not interview the accused employee, except where, in the opinion of the General Counsel, there are exigent circumstances⁵ which require that the employee be interviewed. If such exigent circumstances exist, the General Counsel or other attorney in the General Counsel's office may interview the accused employee to the extent reasonably necessary to eliminate or substantially reduce the exigency.

(3) In all other cases of alleged serious felonies, the General Counsel, or the General Counsel's designee, may interview the accused employee only after consultation with the Agency's IG, a Defense Criminal Investigative Organization (for Defense and military employees), or with the Department of Justice regarding the procedures to be used during an interview with the accused employee.

Any interview of an accused employee that is undertaken shall be conducted in a manner that does not cause the loss, concealment, destruction, damage or alteration of evidence of the alleged crime, nor result in the immunization of any statements made by the accused employee during that interview. The Agency shall not otherwise be limited by this MOU either as to the techniques it is otherwise authorized to use, or as to its responsibility to provide for its security functions pursuant to E.O. 12333.

⁴ A "serious felony offense" includes any offense listed in Section VII, hereof, violent crimes, and other offenses which, if committed in the presence of a reasonably prudent and law-abiding person, would cause that person immediately to report that conduct directly to the police. For purposes of this MOU, crimes against government property that do not exceed \$5,000 and are not part of a pattern of continuing behavior or of a criminal conspiracy shall not be considered serious felony offenses.

⁵ "Exigent circumstances" are circumstances requiring prompt action by the Agency in order to protect life or substantial property interests; to apprehend or identify a fleeing offender; or to prevent the compromise, loss, concealment, destruction, or alteration of evidence in a crime.

VI. GENERAL CONSIDERATIONS: ALLEGATIONS OF CRIMINAL ACTS COMMITTED BY NON-EMPLOYEES

(A) This MOU requires each employee of the Agency to report, to the General Counsel or as otherwise directed by the Department or Agency head, facts or circumstances that reasonably indicate to the employee that a non-employee has committed, is committing, or will commit one or more of the specified crimes in Section VII, below.

(B) When an Agency has received information concerning alleged violations of federal law by a person other than an employee of an intelligence agency, and has determined that the reported information provides a reasonable basis to conclude that a violation of one of the specified crimes in Section VII has occurred, is occurring, or may occur, the Agency shall report that information to the Department of Justice in accordance with Sections VIII or IX, below.

VII. REPORTABLE OFFENSES BY NON-EMPLOYEES

(A) Unless exempted under Section III, above, allegations concerning criminal activities by non-employees are reportable if they pertain to one or more of the following specified violations of federal criminal law:

(1) Crimes involving intentional infliction or threat of death or serious physical harm. These include but are not limited to homicide, kidnapping, hostage taking, assault (including sexual assault), or threats or attempts to commit such offenses, against any person in the United States or a U.S. national or internationally protected person (as defined in 18 U.S.C. § 1116(b)(4)), whether in the United States or abroad.

(2) Crimes, including acts of terrorism, that are likely to affect the national security, defense or foreign relations of the United States. These may include but are not limited to:

(a) Espionage; sabotage; unauthorized disclosure of classified information; seditious conspiracies to overthrow the government of the United States; fund transfers violating the International Emergency Economic Powers Act; providing material or financial support to terrorists; unauthorized traffic in controlled munitions or technology; or unauthorized traffic in, use of, or contamination by nuclear materials, chemical or biological weapons, or chemical or biological agents; whether in the United States or abroad;

(b) Fraudulent entry of persons into the United States, the violation of immigration restrictions or the failure to register as a foreign agent or an intelligence trained agent;

(c) Offenses involving interference with foreign governments or interference with the foreign policy of the United States whether occurring in the United States or abroad;

(d) Acts of terrorism anywhere in the world which target the U.S. government or its property, U.S. persons, or any property in the United States, or in which the perpetrator is a U.S. person; aircraft hijacking; attacks on aircraft or international aviation facilities; or maritime piracy;

(e) The unauthorized transportation or use of firearms or explosives in interstate or foreign commerce.

(3) Crimes involving foreign interference with the integrity of U.S. governmental institutions or processes. Such crimes may include:

(a) Activities to defraud the U.S. government or any federally protected financial institution, whether occurring in the United States or abroad;

(b) Obstruction of justice or bribery of U.S. officials or witnesses in U.S. proceedings, whether occurring in the United States or abroad;

(c) Interference with U.S. election proceedings or illegal contributions by foreign persons to U.S. candidates or election committees;

(d) Perjury in connection with U.S. proceedings, or false statements made in connection with formal reports or applications to the U.S. government, or in connection with a formal criminal or administrative investigation, whether committed in the United States or abroad;

(e) Counterfeiting U.S. obligations or any other governmental currency, security or identification documents used in the United States, whether committed in the United States or abroad; transactions involving stolen governmental securities or identification documents or stolen or counterfeit non-governmental securities.

(4) Crimes related to unauthorized electronic surveillance in the United States or to tampering with, or unauthorized access to, computer systems.

(5) Violations of U.S. drug laws including: the cultivation, production, transportation, importation, sale, or possession (other than possession of user quantities) of controlled substances; the production, transportation, importation, and sale of precursor or essential chemicals.

(6) The transmittal, investment and/or laundering of the proceeds of any of the unlawful activities listed in this Section, whether committed in the United States or abroad.

(B) Any conspiracy or attempt to commit a crime reportable under this section shall be reported if the conspiracy or attempt itself meets the applicable reporting criteria.

(C) The Attorney General also encourages the Agency to notify the Department of Justice when the Agency's otherwise routine collection of intelligence in accordance with its authorities results in its acquisition of information about the commission of other serious felony offenses by non-employees, e.g. violations of U.S. environmental laws relating to ocean and inland water discharging or dumping, drinking water contamination, or hazardous waste disposal, and crimes involving interference with the integrity of U.S. governmental institutions or processes that would not otherwise be reportable under section VII.A.3.

VIII. PROCEDURE FOR SUBMITTING SPECIAL CRIMES REPORTS

(A) Where the Agency determines that a matter must be the subject of a special report to the Department of Justice, it may, consistent with paragraphs VIII.B and VIII.C, below, make such a report (1) by letter or other, similar communication from the General Counsel, or (2) by electronic or courier dissemination of information from operational or analytical units, provided that in all cases, the subject line and the text of such communication or dissemination clearly reflects that it is a report of possible criminal activity. The Department of Justice shall maintain a record of all special crimes reports received from the Agency.

(B) Where the Agency determines that a matter must be the subject of a special report to the Department of Justice; and where the Agency further determines that no public disclosure of classified information or intelligence sources and methods would result from further investigation or prosecution, and the security of ongoing intelligence operations would not be jeopardized thereby, the Agency will report the matter to the federal investigative agency having jurisdiction over the criminal matter. A copy of that report must also be provided to the AAG, or designated Deputy AAG, Criminal Division.

(C) Where the Agency determines that further investigation or prosecution of a matter that must be specifically reported may result in a public disclosure of classified information or intelligence sources or methods or would jeopardize the security of ongoing intelligence operations, the Agency shall report the matter to the AAG or designated Deputy AAG, Criminal Division. A copy of that report must also be provided to the Assistant Director, Criminal Investigations or National Security Divisions, Federal Bureau of Investigation, or in the event that the principal investigative responsibility resides with a different federal investigative agency, to an appropriately cleared person of equivalent position in such agency. The Agency's report should explain the security or operational problems that would or might arise from a criminal investigation or prosecution.

(D) Written documents associated with the reports submitted pursuant to this section may refer to persons who are the subjects of the reports by non-identifying terms (such as "John Doe # ____"). The Agency shall advise the

Department of Justice or relevant federal investigative agency of the true identities of such persons if so requested.

(E) It is agreed that, in acting upon information reported in accordance with these procedures, the Agency, the Department of Justice and the relevant federal investigative agencies will deal with classified information, including sources and methods, in a manner consistent with the provisions of relevant statutes and Executive Orders, including the Classified Information Procedures Act.

IX. WHEN ROUTINE DISSEMINATION MAY BE USED IN LIEU OF A SPECIAL CRIMES REPORT

(A) Except as set forth in IX.B, below, the Agency may report crimes information regarding non-employees to the Department of Justice by routine dissemination, provided that:

- (1) the crimes information is of the type that is routinely disseminated by the Agency to headquarters elements of cognizant federal investigative agencies;
- (2) the criminal activity is of a kind that is normally collected and disseminated to law enforcement by the Agency (e.g., drug trafficking, money laundering, terrorism, or sanctions violations); and
- (3) the persons or entities involved are members of a class that are routinely the targets or objects of such collection and dissemination.

If all three of these conditions are met, the Agency may satisfy its crimes reporting obligation through routine dissemination to the Department of Justice, Criminal Division, and to all cognizant federal law enforcement agencies, which shall retain primary responsibility for review of disseminated information for evidence of criminal activity. In all other cases, the special reporting procedures in Section VIII shall apply. As requested by the Department of Justice, the Agency will coordinate with the Department to facilitate the Department's analytical capabilities as to the Agency's routine dissemination of crimes information in compliance with this MOU.

(B) Routine dissemination, as discussed in IX.A, above, may not be used in lieu of the special reporting requirements set forth herein as to the following categories of criminal activities:

- (1) Certain crimes involving the intentional infliction or threat of death or serious physical harm (VII.A.1, above);
- (2) Espionage; sabotage; unauthorized disclosure of classified information; and seditious conspiracies to overthrow the government of the United States (VII.A.2.a, above); and
- (3) Certain crimes involving foreign interference with the integrity of U.S. governmental institutions or processes (VII.A.3.b and c, above).

X. OTHER AGENCY RESPONSIBILITIES

(A) The Agency shall develop internal procedures in accordance with the provisions of Sections VIII and IX for the reporting of criminal information by its employees as required under Sections IV.A and VI.A.

(B) The Agency shall also establish initial and continuing training to ensure that its employees engaged in the review and analysis of collected intelligence are knowledgeable of and in compliance with the provisions of this MOU.

XI. RELATION TO OTHER PROCEDURES AND AGREEMENTS

(A) If the Agency desires, for administrative or security reasons, to conduct a more extensive investigation into the activities of an employee relating to any matter reported pursuant to this MOU, it will inform the Department of Justice and the federal investigative agency to which the matter was reported. The Agency may also take appropriate administrative, disciplinary, or other adverse action at any time against any employee whose activities are reported under these procedures. However, such investigations or adverse actions shall be coordinated with the proper investigative or prosecuting officials to avoid prejudice to any criminal investigation or prosecution.

(B) Nothing in these procedures shall be construed to restrict the exchange of information among the Agencies in the Intelligence Community or between those Agencies and law enforcement entities other than the Department of Justice.

(C) This MOU supersedes all prior crimes reporting memoranda of understanding executed pursuant to the requirements of E.O. 12333. To the extent that there exist any conflicts between other Agency policies or directives and the provisions herein, such conflicts shall be resolved in accordance with the provisions of this MOU. However, this MOU shall not be construed to modify in any way the August 1984 Memorandum of Understanding between the Department of Defense and the Department of Justice relating to the investigation and prosecution of certain crimes.

(D) The parties understand and agree that nothing herein shall be construed to alter in any way the current routine dissemination by the Agency of intelligence information, including information regarding alleged criminal activities by any person, to the Department of Justice or to federal law enforcement agencies.

XII. MISCELLANEOUS

(A) This MOU shall become effective as to each agency below as of the date signed by the listed representative of that agency.

(B) The Intelligence-Law Enforcement Policy Board, within one year of the date of the effective date hereof, and as it deems appropriate thereafter, will appoint a working group consisting of an equal number of representatives from the

MOU: REPORTING OF INFORMATION CONCERNING FEDERAL CRIMES

intelligence and law enforcement communities, including the Criminal Division. That working group shall do the following:

- (1) review the Agency's implementation of Sections III.F and IV.B, hereof;
- (2) consider whether the crimes reporting requirements of E.O. 12333 and other authorities are being met through the operation of this MOU;
- (3) review each of the provisions of this MOU and determine what, if any, modifications thereof should be recommended to the Policy Board, or its successor; and
- (4) issue a report to the Policy Board of its findings and recommendations in each of the foregoing categories.

(C) The Policy Board in turn shall make recommendations to the Attorney General, the Director of Central Intelligence, and the heads of the affected agencies concerning any modifications to the MOU that it considers necessary.

-/S/-Janet Reno
Attorney General
Date: August 3, 1995

-/S/-William J. Perry
Secretary of Defense
Date: 11 AUG 1995

-/S/-John Deutch
Director of Central Intelligence
Date: 3 August 1995

-/S/-JM McConnell
Director, National Security Agency
Date: 22 Aug 1995

-/S/-Michael F. Munson
Director, Defense Intelligence
Intelligence Agency
Date: 2 Aug 1995

-/S/-Toby T. Gati
Assistant Secretary of State,
Intelligence and Research
Date: 8/14/95

-/S/-Kenneth E. Baker
Director, Office Of Non-Proliferation
and National Security,
Department of Energy
Date: 15 Aug 95

INTELLIGENCE COMMUNITY AND GOVERNMENT WEBSITES

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE: www.dni.gov
NATIONAL COUNTERTERRORISM CENTER: www.nctc.gov
NATIONAL COUNTERINTELLIGENCE AND SECURITY CENTER: www.ncsc.gov
PROGRAM MANAGER, INFORMATION SHARING ENVIRONMENT: www.ise.gov
INTELLIGENCE COMMUNITY LEGAL REFERENCE BOOK: www.dni.gov/ogc
IC ON THE RECORD: www.icontherecord.tumblr.com

CENTRAL INTELLIGENCE AGENCY: www.cia.gov

NATIONAL SECURITY AGENCY: www.nsa.gov

DEFENSE INTELLIGENCE AGENCY: www.dia.mil

NATIONAL GEOSPATIAL-INTELLIGENCE AGENCY: www.nga.mil

NATIONAL RECONNAISSANCE OFFICE: www.nro.gov

DEPARTMENT OF DEFENSE: www.defenselink.mil; www.defense.gov

ARMY: www.army.mil

INSCOM: www.inscom.army.mil

NAVY: www.navy.mil

ONI: www.oni.navy.mil

MARINE CORPS: www.marines.mil

USMC INTELLIGENCE:

www.hqmc.marines.mil/intelligence/UnitHome.aspx

AIR FORCE: www.af.mil

AF ISR AGENCY: www.afisr.af.mil

SPACE FORCE: www.spaceforce.mil

DEPARTMENT OF JUSTICE: www.usdoj.gov

FBI: www.fbi.gov

DEA: www.dea.gov

OLC: www.usdoj.gov/olc

NSD: www.usdoj.gov/nsd

DEPARTMENT OF STATE: www.state.gov

DEPARTMENT OF TREASURY: www.treasury.gov

DEPARTMENT OF HOMELAND SECURITY: www.dhs.gov

COAST GUARD: www.uscg.mil

HOMELAND SECURITY DIGITAL LIBRARY: www.hsdl.org

DEPARTMENT OF ENERGY: www.energy.gov

WHITE HOUSE: www.whitehouse.gov

U.S. SENATE: www.senate.gov

SELECT COMMITTEE ON INTELLIGENCE: intelligence.senate.gov

JUDICIARY COMMITTEE: judiciary.senate.gov

ARMED SERVICES COMMITTEE: armed-services.senate.gov

FOREIGN RELATIONS COMMITTEE: foreign.senate.gov

HOMELAND SECURITY & GOVERNMENTAL AFFAIRS COMMITTEE:

hsgac.senate.gov/public

U.S. HOUSE OF REPRESENTATIVES: www.house.gov

PERMANENT SELECT COMMITTEE ON INTELLIGENCE: intelligence.house.gov

JUDICIARY COMMITTEE: judiciary.house.gov

ARMED SERVICES COMMITTEE: armedservices.house.gov

FOREIGN AFFAIRS: foreignaffairs.house.gov

HOMELAND SECURITY: homeland.house.gov

OVERSIGHT & GOVERNMENT REFORM: oversight.house.gov

LIBRARY OF CONGRESS: www.congress.gov

BONUS DIGITAL ONLY CONTENT

**PROCEDURES FOR THE RETENTION OF INCIDENTALY
ACQUIRED COMMUNICATIONS**

**PROCEDURES FOR THE RETENTION OF INCIDENTALY
ACQUIRED COMMUNICATIONS**

[Public Law 113–293; 128 STAT. 3998; December 19, 2014]

SEC. 309 OF THE INTELLIGENCE AUTHORIZATION ACT FOR FISCAL YEAR 2015
[50 U.S.C. § 1813].

(a) DEFINITIONS.—In this section:

(1) COVERED COMMUNICATION.—The term “covered communication” means any nonpublic telephone or electronic communication acquired without the consent of a person who is a party to the communication, including communications in electronic storage.

(2) HEAD OF AN ELEMENT OF THE INTELLIGENCE COMMUNITY.—The term “head of an element of the intelligence community” means, as appropriate—

(A) the head of an element of the intelligence community; or

(B) the head of the department or agency containing such element.

(3) UNITED STATES PERSON.—The term “United States person” has the meaning given that term in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801).

(b) PROCEDURES FOR COVERED COMMUNICATIONS.—

(1) REQUIREMENT TO ADOPT.—Not later than 2 years after the date of the enactment of this Act each head of an element of the intelligence community shall adopt procedures approved by the Attorney General for such element that ensure compliance with the requirements of paragraph (3).

(2) COORDINATION AND APPROVAL.—The procedures required by paragraph (1) shall be—

(A) prepared in coordination with the Director of National Intelligence; and

(B) approved by the Attorney General prior to issuance.

(3) PROCEDURES.—

(A) APPLICATION.—The procedures required by paragraph (1) shall apply to any intelligence collection activity not otherwise authorized by court order (including an order or certification issued by a court established under subsection (a) or (b) of section 103 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1803)), subpoena, or similar legal process that is

**PROCEDURES FOR THE RETENTION OF INCIDENTALLY
ACQUIRED COMMUNICATIONS**

reasonably anticipated to result in the acquisition of a covered communication to or from a United States person and shall permit the acquisition, retention, and dissemination of covered communications subject to the limitation in subparagraph (B). (B) LIMITATION ON RETENTION.—A covered communication shall not be retained in excess of 5 years, unless—

- (i) the communication has been affirmatively determined, in whole or in part, to constitute foreign intelligence or counterintelligence or is necessary to understand or assess foreign intelligence or counterintelligence;
- (ii) the communication is reasonably believed to constitute evidence of a crime and is retained by a law enforcement agency;
- (iii) the communication is enciphered or reasonably believed to have a secret meaning;
- (iv) all parties to the communication are reasonably believed to be non-United States persons;
- (v) retention is necessary to protect against an imminent threat to human life, in which case both the nature of the threat and the information to be retained shall be reported to the congressional intelligence committees not later than 30 days after the date such retention is extended under this clause;
- (vi) retention is necessary for technical assurance or compliance purposes, including a court order or discovery obligation, in which case access to information retained for technical assurance or compliance purposes shall be reported to the congressional intelligence committees on an annual basis; or
- (vii) retention for a period in excess of 5 years is approved by the head of the element of the intelligence community responsible for such retention, based on a determination that retention is necessary to protect the national security of the United States, in which case the head of such element shall provide to the congressional intelligence committees a written certification describing—

**PROCEDURES FOR THE RETENTION OF INCIDENTALY
ACQUIRED COMMUNICATIONS**

- (I) the reasons extended retention is necessary to protect the national security of the United States;
- (II) the duration for which the head of the element is authorizing retention;
- (III) the particular information to be retained;
- and
- (IV) the measures the element of the intelligence community is taking to protect the privacy interests of United States persons or persons located inside the United States.

TITLE 10, CHAPTER 47A, UNITED STATES CODE,
MILITARY COMMISSIONS

TABLE OF CONTENTS

SUBCHAPTER I—GENERAL PROVISION

- SEC. 948a. Definitions.
- SEC. 948b. Military commissions generally.
- SEC. 948c. Persons subject to military commissions.
- SEC. 948d. Jurisdiction of military commissions.

SUBCHAPTER II—COMPOSITION OF MILITARY COMMISSIONS

- SEC. 948h. Who may convene military commissions.
- SEC. 948i. Who may serve on military commissions.
- SEC. 948j. Military judge of a military commission.
- SEC. 948k. Detail of trial counsel and defense counsel.
- SEC. 948l. Detail or employment of reporters and interpreters.
- SEC. 948m. Number of members; excuse of members; absent and additional members.

SUBCHAPTER III—PRE-TRIAL PROCEDURE

- SEC. 948q. Charges and specifications.
- SEC. 948r. Exclusion of statements obtained by torture or cruel, inhuman, or degrading treatment; prohibition of self-incrimination; admission of other statements of the accused.
- SEC. 948s. Service of charges.

SUBCHAPTER IV—TRIAL PROCEDURE

- SEC. 949a. Rules.
- SEC. 949b. Unlawfully influencing action of military commission and United States Court of Military Commission Review.
- SEC. 949c. Duties of trial counsel and defense counsel.
- SEC. 949d. Sessions.
- SEC. 949e. Continuances.
- SEC. 949f. Challenges.
- SEC. 949g. Oaths.
- SEC. 949h. Former jeopardy.

TITLE 10, MILITARY COMMISSIONS

- SEC. 949i. Pleas of the accused.
- SEC. 949j. Opportunity to obtain witnesses and other evidence.
- SEC. 949k. Defense of lack of mental responsibility.
- SEC. 949l. Voting and rulings.
- SEC. 949m. Number of votes required.
- SEC. 949n. Military commission to announce action.
- SEC. 949o. Record of trial.

SUBCHAPTER V—CLASSIFIED INFORMATION PROCEDURES

- SEC. 949p-1. Protection of classified information: applicability of subchapter.
- SEC. 949p-2. Pretrial conference.
- SEC. 949p-3. Protective orders.
- SEC. 949p-4. Discovery of, and access to, classified information by the accused.
- SEC. 949p-5. Notice by accused of intention to disclose classified information.
- SEC. 949p-6. Procedure for cases involving classified information.
- SEC. 949p-7. Introduction of classified information into evidence.

SUBCHAPTER VI—SENTENCES

- SEC. 949s. Cruel or unusual punishments prohibited.
- SEC. 949t. Maximum limits.
- SEC. 949u. Execution of confinement.

SUBCHAPTER VII—POST-TRIAL PROCEDURE AND REVIEW OF MILITARY COMMISSIONS

- SEC. 950a. Error of law; lesser included offense.
- SEC. 950b. Review by the convening authority.
- SEC. 950c. Appellate referral; waiver or withdrawal of appeal.
- SEC. 950d. Interlocutory appeals by the United States.
- SEC. 950e. Rehearings.
- SEC. 950f. Review by United States Court of Military Commission Review.
- SEC. 950g. Review by United States Court of Appeals for the District of Columbia Circuit; writ of certiorari to Supreme Court.
- SEC. 950h. Appellate counsel.
- SEC. 950i. Execution of sentence; suspension of sentence.
- SEC. 950j. Finality of proceedings, findings, and sentences.

TITLE 10, MILITARY COMMISSIONS

SUBCHAPTER VIII—PUNITIVE MATTERS

- SEC. 950p. Definitions; construction of certain offenses; common circumstances.
- SEC. 950q. Principals.
- SEC. 950r. Accessory after the fact.
- SEC. 950s. Conviction of lesser offenses.
- SEC. 950t. Crimes triable by military commission.

SUBCHAPTER I – GENERAL PROVISIONS

DEFINITIONS

SEC. 948A.

In this chapter:

- (1) ALIEN.—The term “alien” means an individual who is not a citizen of the United States.
- (2) CLASSIFIED INFORMATION.—The term “classified information” means the following:
 - (A) Any information or material that has been determined by the United States Government pursuant to statute, Executive order, or regulation to require protection against unauthorized disclosure for reasons of national security.
 - (B) Any restricted data, as that term is defined in section 11 y. of the Atomic Energy Act of 1954 (42 U.S.C. 2014(y)).
- (3) COALITION PARTNER.—The term “coalition partner”, with respect to hostilities engaged in by the United States, means any State or armed force directly engaged along with the United States in such hostilities or providing direct operational support to the United States in connection with such hostilities.
- (4) GENEVA CONVENTION RELATIVE TO THE TREATMENT OF PRISONERS OF WAR.—The term “Geneva Convention Relative to the Treatment of Prisoners of War” means the Convention Relative to the Treatment of Prisoners of War, done at Geneva August 12, 1949 (6 UST 3316).
- (5) GENEVA CONVENTIONS.—The term “Geneva Conventions” means the international conventions signed at Geneva on August 12, 1949.
- (6) PRIVILEGED BELLIGERENT.—The term “privileged belligerent” means an individual belonging to one of the eight categories enumerated in Article 4 of the Geneva Convention Relative to the Treatment of Prisoners of War.
- (7) UNPRIVILEGED ENEMY BELLIGERENT.—The term “unprivileged enemy belligerent” means an individual (other than a privileged belligerent) who—
 - (A) has engaged in hostilities against the United States or its coalition partners;

(B) has purposefully and materially supported hostilities against the United States or its coalition partners; or

(C) was a part of al Qaeda at the time of the alleged offense under this chapter.

(8) NATIONAL SECURITY.—The term “national security” means the national defense and foreign relations of the United States.

(9) HOSTILITIES.—The term “hostilities” means any conflict subject to the laws of war.

MILITARY COMMISSIONS GENERALLY

SEC. 948B.

(a) PURPOSE.—This chapter establishes procedures governing the use of military commissions to try alien unprivileged enemy belligerents for violations of the law of war and other offenses triable by military commission.

(b) AUTHORITY FOR MILITARY COMMISSIONS UNDER THIS CHAPTER.—The President is authorized to establish military commissions under this chapter for offenses triable by military commission as provided in this chapter.

(c) CONSTRUCTION OF PROVISIONS.—The procedures for military commissions set forth in this chapter are based upon the procedures for trial by general courts-martial under chapter 47 of this title (the Uniform Code of Military Justice). Chapter 47 of this title does not, by its terms, apply to trial by military commission except as specifically provided therein or in this chapter, and many of the provisions of chapter 47 of this title are by their terms inapplicable to military commissions. The judicial construction and application of chapter 47 of this title, while instructive, is therefore not of its own force binding on military commissions established under this chapter.

(d) INAPPLICABILITY OF CERTAIN PROVISIONS.—

(1) The following provisions of this title shall not apply to trial by military commission under this chapter:

(A) Section 810 (article 10 of the Uniform Code of Military Justice), relating to speedy trial, including any rule of courts-martial relating to speedy trial.

(B) Sections 831(a), (b), and (d) (articles 31(a), (b), and (d) of the Uniform Code of Military Justice), relating to compulsory self-incrimination.

(C) Section 832 (article 32 of the Uniform Code of Military Justice), relating to preliminary hearing.

(2) Other provisions of chapter 47 of this title shall apply to trial by military commission under this chapter only to the extent provided by the terms of such provisions or by this chapter.

(e) GENEVA CONVENTIONS NOT ESTABLISHING PRIVATE RIGHT OF ACTION.— No alien unprivileged enemy belligerent subject to trial by military commission under this chapter may invoke the Geneva Conventions as a basis for a private right of action.

PERSONS SUBJECT TO MILITARY COMMISSIONS

SEC. 948C.

Any alien unprivileged enemy belligerent is subject to trial by military commission as set forth in this chapter.

JURISDICTION OF MILITARY COMMISSIONS

SEC. 948D.

A military commission under this chapter shall have jurisdiction to try persons subject to this chapter for any offense made punishable by this chapter, sections 904 and 906 of this title (articles 104 and 106 of the Uniform Code of Military Justice), or the law of war, whether such offense was committed before, on, or after September 11, 2001, and may, under such limitations as the President may prescribe, adjudge any punishment not forbidden by this chapter, including the penalty of death when specifically authorized under this chapter. A military commission is a competent tribunal to make a finding sufficient for jurisdiction.

SUBCHAPTER II—COMPOSITION OF MILITARY COMMISSIONS

WHO MAY CONVENE MILITARY COMMISSIONS

SEC. 948H.

Military commissions under this chapter may be convened by the Secretary of Defense or by any officer or official of the United States designated by the Secretary for that purpose.

WHO MAY SERVE ON MILITARY COMMISSIONS

SEC. 948I.

(a) IN GENERAL.—Any commissioned officer of the armed forces on active duty is eligible to serve on a military commission under this chapter, including commissioned officers of the reserve components of the armed forces on active duty, commissioned officers of the National Guard on active duty in Federal service, or retired commissioned officers recalled to active duty.

(b) **DETAIL OF MEMBERS.**—When convening a military commission under this chapter, the convening authority shall detail as members thereof such members of the armed forces eligible under subsection (a) who, in the opinion of the convening authority, are best qualified for the duty by reason of age, education, training, experience, length of service, and judicial temperament. No member of an armed force is eligible to serve as a member of a military commission when such member is the accuser or a witness for the prosecution or has acted as an investigator or counsel in the same case.

(c) **EXCUSE OF MEMBERS.**—Before a military commission under this chapter is assembled for the trial of a case, the convening authority may excuse a member from participating in the case.

MILITARY JUDGE OF A MILITARY COMMISSION

SEC. 948J.

(a) **DETAIL OF MILITARY JUDGE.**—A military judge shall be detailed to each military commission under this chapter. The Secretary of Defense shall prescribe regulations providing for the manner in which military judges are so detailed to military commissions. The military judge shall preside over each military commission to which such military judge has been detailed.

(b) **ELIGIBILITY.**—A military judge shall be a commissioned officer of the armed forces who is a member of the bar of a Federal court, or a member of the bar of the highest court of a State, and who is certified to be qualified for duty under section 826 of this title (article 26 of the Uniform Code of Military Justice) as a military judge of general courts-martial by the Judge Advocate General of the armed force of which such military judge is a member.

(c) **INELIGIBILITY OF CERTAIN INDIVIDUALS.**—No person is eligible to act as military judge in a case of a military commission under this chapter if such person is the accuser or a witness or has acted as investigator or a counsel in the same case.

(d) **CONSULTATION WITH MEMBERS; INELIGIBILITY TO VOTE.**—A military judge detailed to a military commission under this chapter may not consult with the members except in the presence of the accused (except as otherwise provided in section 949d of this title), trial counsel, and defense counsel, nor may such military judge vote with the members.

(e) **OTHER DUTIES.**—A commissioned officer who is certified to be qualified for duty as a military judge of a military commission under this chapter may perform such other duties as are assigned to such officer by or with the approval of the Judge Advocate General of the armed force of which such officer is a member or the designee of such Judge Advocate General.

(f) PROHIBITION ON EVALUATION OF FITNESS BY CONVENING AUTHORITY.— The convening authority of a military commission under this chapter may not prepare or review any report concerning the effectiveness, fitness, or efficiency of a military judge detailed to the military commission which relates to such judge's performance of duty as a military judge on the military commission.

DETAIL OF TRIAL COUNSEL AND DEFENSE COUNSEL

SEC. 948k.

(a) DETAIL OF COUNSEL GENERALLY.—

- (1) Trial counsel and military defense counsel shall be detailed for each military commission under this chapter.
- (2) Assistant trial counsel and assistant and associate defense counsel may be detailed for a military commission under this chapter.
- (3) Military defense counsel for a military commission under this chapter shall be detailed as soon as practicable.
- (4) The Secretary of Defense shall prescribe regulations providing for the manner in which trial counsel and military defense counsel are detailed for military commissions under this chapter and for the persons who are authorized to detail such counsel for such military commissions.

(b) TRIAL COUNSEL.—Subject to subsection (e), a trial counsel detailed for a military commission under this chapter shall be—

- (1) a judge advocate (as that term is defined in section 801 of this title (article 1 of the Uniform Code of Military Justice)) who is—
 - (A) a graduate of an accredited law school or a member of the bar of a Federal court or of the highest court of a State; and
 - (B) certified as competent to perform duties as trial counsel before general courts-martial by the Judge Advocate General of the armed force of which such judge advocate is a member; or
- (2) a civilian who is—
 - (A) a member of the bar of a Federal court or of the highest court of a State; and
 - (B) otherwise qualified to practice before the military commission pursuant to regulations prescribed by the Secretary of Defense.

(c) DEFENSE COUNSEL.—

- (1) Subject to subsection (e), a military defense counsel detailed for a military commission under this chapter shall be a judge advocate (as so defined) who is—
 - (A) a graduate of an accredited law school or a member of the bar of a Federal court or of the highest court of a State; and

(B) certified as competent to perform duties as defense counsel before general courts-martial by the Judge Advocate General of the armed force of which such judge advocate is a member.

(2) The Secretary of Defense shall prescribe regulations for the appointment and performance of defense counsel in capital cases under this chapter.

(d) CHIEF PROSECUTOR; CHIEF DEFENSE COUNSEL.—

(1) The Chief Prosecutor in a military commission under this chapter shall meet the requirements set forth in subsection (b)(1).

(2) The Chief Defense Counsel in a military commission under this chapter shall meet the requirements set forth in subsection (c)(1).

(e) INELIGIBILITY OF CERTAIN INDIVIDUALS.—No person who has acted as an investigator, military judge, or member of a military commission under this chapter in any case may act later as trial counsel or military defense counsel in the same case. No person who has acted for the prosecution before a military commission under this chapter may act later in the same case for the defense, nor may any person who has acted for the defense before a military commission under this chapter act later in the same case for the prosecution.

DETAIL OR EMPLOYMENT OF REPORTERS AND INTERPRETERS

SEC. 948L.

(a) COURT REPORTERS.—Under such regulations as the Secretary of Defense may prescribe, the convening authority of a military commission under this chapter shall detail to or employ for the military commission qualified court reporters, who shall prepare a verbatim record of the proceedings of and testimony taken before the military commission.

(b) INTERPRETERS.—Under such regulations as the Secretary of Defense may prescribe, the convening authority of a military commission under this chapter may detail to or employ for the military commission interpreters who shall interpret for the military commission, and, as necessary, for trial counsel and defense counsel for the military commission, and for the accused.

(c) TRANSCRIPT; RECORD.—The transcript of a military commission under this chapter shall be under the control of the convening authority of the military commission, who shall also be responsible for preparing the record of the proceedings of the military commission.

**NUMBER OF MEMBERS; EXCUSE OF MEMBERS;
ABSENT AND ADDITIONAL MEMBERS**

SEC. 948M.

(a) NUMBER OF MEMBERS.—

(1) Except as provided in paragraph (2), a military commission under this chapter shall have at least five primary members and as many alternate members as the convening authority shall detail. Alternate members shall be designated in the order in which they will replace an excused primary member.

(2) In a case in which the accused before a military commission under this chapter may be sentenced to a penalty of death, the military commission shall have the number of primary members prescribed by section 949m(c) of this title.

(b) PRIMARY MEMBERS.—Primary members of a military commission under this chapter are voting members.

(c) ALTERNATE MEMBERS.—

(1) A military commission may include alternate members to replace primary members who are excused from service on the commission.

(2) Whenever a primary member is excused from service on the commission, an alternate member, if available, shall replace the excused primary member and the trial may proceed.

(d) EXCUSE OF MEMBERS.—No primary or alternate member of a military commission under this chapter may be absent or excused after the military commission has been assembled for the trial of a case unless excused—

(1) as a result of challenge;

(2) by the military judge for physical disability or other good cause;

(3) by order of the convening authority for good cause; or

(4) in the case of an alternate member, in order to reduce the number of alternate members required for service on the commission, as determined by the convening authority.

(e) ABSENT AND ADDITIONAL MEMBERS.—Whenever the number of primary members of a military commission under this chapter is reduced below the number of primary members required by subsection (a) and there are no remaining alternate members to replace the excused primary members, the trial may not proceed unless the convening authority details new members sufficient to provide not less than such number. The trial may proceed with the new members present after the recorded evidence previously introduced before the members has been read to the military commission in the presence of the military judge, the accused (except as provided in section 949d of this title), and counsel

for both sides. An alternate member who was present for the introduction of all evidence shall not be considered to be a new or additional member.

SUBCHAPTER III—PRE-TRIAL PROCEDURE

CHARGES AND SPECIFICATIONS

SEC. 948Q.

(a) **CHARGES AND SPECIFICATIONS.**—Charges and specifications against an accused in a military commission under this chapter shall be signed by a person subject to chapter 47 of this title under oath before a commissioned officer of the armed forces authorized to administer oaths and shall state—

- (1) that the signer has personal knowledge of, or reason to believe, the matters set forth therein; and
- (2) that such matters are true in fact to the best of the signer's knowledge and belief.

(b) **NOTICE TO ACCUSED.**—Upon the swearing of the charges and specifications in accordance with subsection (a), the accused shall be informed of the charges and specifications against the accused as soon as practicable.

EXCLUSION OF STATEMENTS OBTAINED BY TORTURE OR CRUEL, INHUMAN, OR DEGRADING TREATMENT; PROHIBITION OF SELF-INCRIMINATION; ADMISSION OF OTHER STATEMENTS OF THE ACCUSED

SEC. 948R.

(a) **EXCLUSION OF STATEMENTS OBTAIN BY TORTURE OR CRUEL, INHUMAN, OR DEGRADING TREATMENT.**—No statement obtained by the use of torture or by cruel, inhuman, or degrading treatment (as defined by section 1003 of the Detainee Treatment Act of 2005 (42 U.S.C. 2000dd)), whether or not under color of law, shall be admissible in a military commission under this chapter, except against a person accused of torture or such treatment as evidence that the statement was made.

(b) **SELF-INCRIMINATION PROHIBITED.**—No person shall be required to testify against himself or herself at a proceeding of a military commission under this chapter.

(c) **OTHER STATEMENTS OF THE ACCUSED.**—A statement of the accused may be admitted in evidence in a military commission under this chapter only if the military judge finds—

- (1) that the totality of the circumstances renders the statement reliable and possessing sufficient probative value; and
- (2) that—

(A) the statement was made incident to lawful conduct during military operations at the point of capture or during closely related active combat engagement, and the interests of justice would best be served by admission of the statement into evidence; or

(B) the statement was voluntarily given.

(d) DETERMINATION OF VOLUNTARINESS.—In determining for purposes of subsection (c)(2)(B) whether a statement was voluntarily given, the military judge shall consider the totality of the circumstances, including, as appropriate, the following:

(1) The details of the taking of the statement, accounting for the circumstances of the conduct of military and intelligence operations during hostilities.

(2) The characteristics of the accused, such as military training, age, and education level.

(3) The lapse of time, change of place, or change in identity of the questioners between the statement sought to be admitted and any prior questioning of the accused.

SERVICE OF CHARGES

SEC. 948S.

The trial counsel assigned to a case before a military commission under this chapter shall cause to be served upon the accused and military defense counsel a copy of the charges upon which trial is to be had in English and, if appropriate, in another language that the accused understands, sufficiently in advance of trial to prepare a defense.

SUBCHAPTER IV—TRIAL PROCEDURE

RULES

SEC. 949A.

(a) PROCEDURES AND RULES OF EVIDENCE.—Pretrial, trial, and post-trial procedures, including elements and modes of proof, for cases triable by military commission under this chapter may be prescribed by the Secretary of Defense. Such procedures may not be contrary to or inconsistent with this chapter. Except as otherwise provided in this chapter or chapter 47 of this title, the procedures and rules of evidence applicable in trials by general courts-martial of the United States shall apply in trials by military commission under this chapter.

(b) EXCEPTIONS.—

(1) In trials by military commission under this chapter, the Secretary of Defense, in consultation with the Attorney General, may make such exceptions in the applicability of the procedures and rules of evidence otherwise applicable in general courts-martial as may be required by the unique circumstances of the conduct of military and intelligence operations during hostilities or by other practical need consistent with this chapter.

(2) Notwithstanding any exceptions authorized by paragraph (1), the procedures and rules of evidence in trials by military commission under this chapter shall include, at a minimum, the following rights of the accused:

(A) To present evidence in the accused's defense, to cross-examine the witnesses who testify against the accused, and to examine and respond to all evidence admitted against the accused on the issue of guilt or innocence and for sentencing, as provided for by this chapter.

(B) To be present at all sessions of the military commission (other than those for deliberations or voting), except when excluded under section 949d of this title.

(C)(i) When none of the charges sworn against the accused are capital, to be represented before a military commission by civilian counsel if provided at no expense to the Government, and by either the defense counsel detailed or the military counsel of the accused's own selection, if reasonably available.

(ii) When any of the charges sworn against the accused are capital, to be represented before a military commission in accordance with clause (i) and, to the greatest extent practicable, by at least one additional counsel who is learned in applicable law relating to capital cases and who, if necessary, may be a civilian and compensated in accordance with regulations prescribed by the Secretary of Defense.

(D) To self-representation, if the accused knowingly and competently waives the assistance of counsel, subject to the provisions of paragraph (4).

(E) To the suppression of evidence that is not reliable or probative.

(F) To the suppression of evidence the probative value of which is substantially outweighed by—

- (i) the danger of unfair prejudice, confusion of the issues, or misleading the members; or
 - (ii) considerations of undue delay, waste of time, or needless presentation of cumulative evidence.
- (3) In making exceptions in the applicability in trials by military commission under this chapter from the procedures and rules otherwise applicable in general courts-martial, the Secretary of Defense may provide the following:
 - (A) Evidence seized outside the United States shall not be excluded from trial by military commission on the grounds that the evidence was not seized pursuant to a search warrant or authorization.
 - (B) A statement of the accused that is otherwise admissible shall not be excluded from trial by military commission on grounds of alleged coercion or compulsory self-incrimination so long as the evidence complies with the provisions of section 948r of this title.
 - (C) Evidence shall be admitted as authentic so long as—
 - (i) the military judge of the military commission determines that there is sufficient evidence that the evidence is what it is claimed to be; and
 - (ii) the military judge instructs the members that they may consider any issue as to authentication or identification of evidence in determining the weight, if any, to be given to the evidence.
 - (D) Hearsay evidence not otherwise admissible under the rules of evidence applicable in trial by general courts-martial may be admitted in a trial by military commission only if—
 - (i) the proponent of the evidence makes known to the adverse party, sufficiently in advance to provide the adverse party with a fair opportunity to meet the evidence, the proponent's intention to offer the evidence, and the particulars of the evidence (including information on the circumstances under which the evidence was obtained); and
 - (ii) the military judge, after taking into account all of the circumstances surrounding the taking of the statement, including the degree to which the statement is corroborated, the indicia of reliability within the statement itself, and whether the will of the declarant was overborne, determines that—

- (I) the statement is offered as evidence of a material fact;
- (II) the statement is probative on the point for which it is offered;
- (III) direct testimony from the witness is not available as a practical matter, taking into consideration the physical location of the witness, the unique circumstances of military and intelligence operations during hostilities, and the adverse impacts on military or intelligence operations that would likely result from the production of the witness; and
- (IV) the general purposes of the rules of evidence and the interests of justice will best be served by admission of the statement into evidence.

(4)(A) The accused in a military commission under this chapter who exercises the right to self-representation under paragraph (2)(D) shall conform the accused's department and the conduct of the defense to the rules of evidence, procedure, and decorum applicable to trials by military commission.

(B) Failure of the accused to conform to the rules described in subparagraph (A) may result in a partial or total revocation by the military judge of the right of self-representation under paragraph (2)(D). In such case, the military counsel of the accused or an appropriately authorized civilian counsel shall perform the functions necessary for the defense.

(c) DELEGATION OF AUTHORITY TO PRESCRIBE REGULATIONS.—The Secretary of Defense may delegate the authority of the Secretary to prescribe regulations under this chapter.

(d) NOTICE TO CONGRESS OF MODIFICATION OF RULES.—Not later than 60 days before the date on which any proposed modification of the rules in effect for military commissions under this chapter goes into effect, the Secretary of Defense shall submit to the Committee on Armed Services of the Senate and the Committee on Armed Services of the House of Representatives a report describing the proposed modification.

UNLAWFULLY INFLUENCING ACTION OF MILITARY COMMISSION AND UNITED STATES COURT OF MILITARY COMMISSION REVIEW

SEC. 949B.

(a) **MILITARY COMMISSIONS.**—

(1) No authority convening a military commission under this chapter may censure, reprimand, or admonish the military commission, or any member, military judge, or counsel thereof, with respect to the findings or sentence adjudged by the military commission, or with respect to any other exercises of its or their functions in the conduct of the proceedings.

(2) No person may attempt to coerce or, by any unauthorized means, influence—

(A) the action of a military commission under this chapter, or any member thereof, in reaching the findings or sentence in any case;

(B) the action of any convening, approving, or reviewing authority with respect to their judicial acts; or

(C) the exercise of professional judgment by trial counsel or defense counsel.

(3) The provisions of this subsection shall not apply with respect to—

(A) general instructional or informational courses in military justice if such courses are designed solely for the purpose of instructing members of a command in the substantive and procedural aspects of military commissions; or

(B) statements and instructions given in open proceedings by a military judge or counsel.

(b) **UNITED STATES COURT OF MILITARY COMMISSION REVIEW.**—

(1) No person may attempt to coerce or, by any unauthorized means, influence—

(A) the action of a judge on the United States Court of Military Commissions Review in reaching a decision on the findings or sentence on appeal in any case; or

(B) the exercise of professional judgment by trial counsel or defense counsel appearing before the United States Court of Military Commission Review.

(2) No person may censure, reprimand, or admonish a judge on the United States Court of Military Commission Review, or counsel thereof, with respect to any exercise of their functions in the conduct of proceedings under this chapter.

- (3) The provisions of this subsection shall not apply with respect to—
- (A) general instructional or informational courses in military justice if such courses are designed solely for the purpose of instructing members of a command in the substantive and procedural aspects of military commissions; or
 - (B) statements and instructions given in open proceedings by a judge on the United States Court of Military Commission Review, or counsel.
- (4) No appellate military judge on the United States Court of Military Commission Review may be reassigned to other duties, except under circumstances as follows:
- (A) The appellate military judge voluntarily requests to be reassigned to other duties and the Secretary of Defense, or the designee of the Secretary, in consultation with the Judge Advocate General of the armed force of which the appellate military judge is a member, approves such reassignment.
 - (B) The appellate military judge retires or otherwise separates from the armed forces.
 - (C) The appellate military judge is reassigned to other duties by the Secretary of Defense, or the designee of the Secretary, in consultation with the Judge Advocate General of the armed force of which the appellate military judge is a member, based on military necessity and such reassignment is consistent with service rotation regulations (to the extent such regulations are applicable).
 - (D) The appellate military judge is withdrawn by the Secretary of Defense, or the designee of the Secretary, in consultation with the Judge Advocate General of the armed force of which the appellate military judge is a member, for good cause consistent with applicable procedures under chapter 47 of this title (the Uniform Code of Military Justice).

(c) PROHIBITION ON CONSIDERATION OF ACTIONS ON COMMISSION IN EVALUATION OF FITNESS.—In the preparation of an effectiveness, fitness, or efficiency report or any other report or document used in whole or in part for the purpose of determining whether a commissioned officer of the armed forces is qualified to be advanced in grade, or in determining the assignment or transfer of any such officer or whether any such officer should be retained on active duty, no person may—

- (1) consider or evaluate the performance of duty of any member of a military commission under this chapter; or

(2) give a less favorable rating or evaluation to any commissioned officer because of the zeal with which such officer, in acting as counsel, represented any accused before a military commission under this chapter.

DUTIES OF TRIAL COUNSEL AND DEFENSE COUNSEL

SEC. 949C.

(a) **TRIAL COUNSEL.**—The trial counsel of a military commission under this chapter shall prosecute in the name of the United States.

(b) **DEFENSE COUNSEL.**—

(1) The accused shall be represented in the accused's defense before a military commission under this chapter as provided in this subsection.

(2) The accused may be represented by military counsel detailed under section 948k of this title or by military counsel of the accused's own selection, if reasonably available.

(3) The accused may be represented by civilian counsel if retained by the accused, provided that such civilian counsel—

(A) is a United States citizen;

(B) is admitted to the practice of law in a State, district, or possession of the United States, or before a Federal court;

(C) has not been the subject of any sanction of disciplinary action by any court, bar, or other competent governmental authority for relevant misconduct;

(D) has been determined to be eligible for access to information classified at the level Secret or higher; and

(E) has signed a written agreement to comply with all applicable regulations or instructions for counsel, including any rules of court for conduct during the proceedings.

(4) If the accused is represented by civilian counsel, military counsel shall act as associate counsel.

(5) The accused is not entitled to be represented by more than one military counsel. However, the person authorized under regulations prescribed under section 948k of this title to detail counsel, in such person's sole discretion, may detail additional military counsel to represent the accused.

(6) Defense counsel may cross-examine each witness for the prosecution who testifies before a military commission under this chapter.

(7) Civilian defense counsel shall protect any classified information received during the course of representation of the accused in accordance with all applicable law governing the protection of classified

information, and may not divulge such information to any person not authorized to receive it.

SESSIONS

SEC. 949D.

(a) SESSIONS WITHOUT PRESENCE OF MEMBERS.—

(1) At any time after the service of charges which have been referred for trial by military commission under this chapter, the military judge may call the military commission into session without the presence of the members for the purpose of—

- (A) hearing and determining motions raising defenses or objections which are capable of determination without trial of the issues raised by a plea of not guilty;
- (B) hearing and ruling upon any matter which may be ruled upon by the military judge under this chapter, whether or not the matter is appropriate for later consideration or decision by the members;
- (C) if permitted by regulations prescribed by the Secretary of Defense, receiving the pleas of the accused; and
- (D) performing any other procedural function which may be performed by the military judge under this chapter or under rules prescribed pursuant to section 949a of this title and which does not require the presence of the members.

(2) Except as provided in subsections (b), (c), and (d), any proceedings under paragraph (1) shall be conducted in the presence of the accused, defense counsel, and trial counsel, and shall be made part of the record.

(b) DELIBERATION OR VOTE OF MEMBERS.—When the members of a military commission under this chapter deliberate or vote, only the members may be present.

(c) CLOSURE OF PROCEEDINGS.—

(1) The military judge may close to the public all or part of the proceedings of a military commission under this chapter.

(2) The military judge may close to the public all or a portion of the proceedings under paragraph (1) only upon making a specific finding that such closure is necessary to—

- (A) protect information the disclosure of which could reasonably be expected to cause damage to the national security, including intelligence or law enforcement sources, methods, or activities; or
- (B) ensure the physical safety of individuals.

TITLE 10, MILITARY COMMISSIONS

(3) A finding under paragraph (2) may be based upon a presentation, including a presentation ex parte or in camera, by either trial counsel or defense counsel.

(d) EXCLUSION OF ACCUSED FROM CERTAIN PROCEEDINGS.—The military judge may exclude the accused from any portion of a proceeding upon a determination that, after being warned by the military judge, the accused persists in conduct that justifies exclusion from the courtroom—

- (1) to ensure the physical safety of individuals; or
- (2) to prevent disruption of the proceedings by the accused.

CONTINUANCES

SEC. 949E.

The military judge in a military commission under this chapter may, for reasonable cause, grant a continuance to any party for such time, and as often, as may appear to be just.

CHALLENGES

SEC. 949F.

(a) CHALLENGES AUTHORIZED.—The military judge and primary or alternate members of a military commission under this chapter may be challenged by the accused or trial counsel for cause stated to the military commission. The military judge shall determine the relevance and validity of challenges for cause, and may not receive a challenge to more than one person at a time. Challenges by trial counsel shall ordinarily be presented and decided before those by the accused are offered.

(b) PEREMPTORY CHALLENGES.—The accused and trial counsel are each entitled to one peremptory challenge, but the military judge may not be challenged except for cause. Nothing in this section prohibits the military judge from awarding to each party such additional peremptory challenges as may be required in the interests of justice.

(c) CHALLENGES AGAINST ADDITIONAL MEMBERS.—Whenever additional members are detailed to a military commission under this chapter, and after any challenges for cause against such additional members are presented and decided, the accused and trial counsel are each entitled to one peremptory challenge against members not previously subject to peremptory challenge.

OATHS

SEC. 949G.

(a) IN GENERAL.—

(1) Before performing their respective duties in a military commission under this chapter, military judges, members, trial counsel, defense counsel, reporters, and interpreters shall take an oath to perform their duties faithfully.

(2) The form of the oath required by paragraph (1), the time and place of the taking thereof, the manner of recording thereof, and whether the oath shall be taken for all cases in which duties are to be performed or for a particular case, shall be as provided in regulations prescribed by the Secretary of Defense. The regulations may provide that—

(A) an oath to perform faithfully duties as a military judge, trial counsel, or defense counsel may be taken at any time by any judge advocate or other person certified to be qualified or competent for the duty; and

(B) if such an oath is taken, such oath need not again be taken at the time the judge advocate or other person is detailed to that duty.

(b) WITNESSES.—Each witness before a military commission under this chapter shall be examined on oath.

(c) OATH DEFINED.—In this section, the term “oath” includes an affirmation.

FORMER JEOPARDY

SEC. 949H.

(a) IN GENERAL.—No person may, without the person’s consent, be tried by a military commission under this chapter a second time for the same offense.

(b) SCOPE OF TRIAL.—No proceeding in which the accused has been found guilty by military commission under this chapter upon any charge or specification is a trial in the sense of this section until the finding of guilty has become final after review of the case has been fully completed.

PLEAS OF THE ACCUSED

SEC. 949I.

(a) PLEA OF NOT GUILTY.—If an accused in a military commission under this chapter after a plea of guilty sets up matter inconsistent with the plea, or if it appears that the accused has entered the plea of guilty through lack of understanding of its meaning and effect, or if the accused fails or refuses to

plead, a plea of not guilty shall be entered in the record, and the military commission shall proceed as though the accused had pleaded not guilty.

(b) **FINDING OF GUILT AFTER GUILTY PLEA.**—With respect to any charge or specification to which a plea of guilty has been made by the accused in a military commission under this chapter and accepted by the military judge, including a charge or specification that has been referred capital, a finding of guilty of the charge or specification may be entered by the military judge immediately without a vote by the members. The finding shall constitute the finding of the military commission unless the plea of guilty is withdrawn prior to announcement of the sentence, in which event the proceedings shall continue as though the accused had pleaded not guilty.

(c) **PRE-TRIAL AGREEMENTS.**—

(1) A plea of guilty made by the accused that is accepted by a military judge under subsection (b) and not withdrawn prior to announcement of the sentence may form the basis for an agreement reducing the maximum sentence approved by the convening authority, including the reduction of a sentence of death to a lesser punishment, or that the case will be referred to a military commission under this chapter without seeking the penalty of death. Such an agreement may provide for terms and conditions in addition to a guilty plea by the accused in order to be effective.

(2) A plea agreement under this subsection may not provide for a sentence of death imposed by a military judge alone. A sentence of death may only be imposed by the unanimous vote of all members of a military commission concurring in the sentence of death as provided in section 949m(b)(2)(D) of this title.

OPPORTUNITY TO OBTAIN WITNESSES AND OTHER EVIDENCE

SEC. 949J.

(a) **IN GENERAL.**—

(1) Defense counsel in a military commission under this chapter shall have a reasonable opportunity to obtain witnesses and other evidence as provided in regulations prescribed by the Secretary of Defense. The opportunity to obtain witnesses and evidence shall be comparable to the opportunity available to a criminal defendant in a court of the United States under article III of the Constitution.

(2) Process issued in military commissions under this chapter to compel witnesses to appear and testify and to compel the production of other evidence—

(A) shall be similar to that which courts of the United States having criminal jurisdiction may lawfully issue; and

(B) shall run to any place where the United States shall have jurisdiction thereof.

(b) DISCLOSURE OF EXCULPATORY EVIDENCE.—

(1) As soon as practicable, trial counsel in a military commission under this chapter shall disclose to the defense the existence of any evidence that reasonably tends to—

(A) negate the guilt of the accused of an offense charged; or

(B) reduce the degree of guilt of the accused with respect to an offense charged.

(2) The trial counsel shall, as soon as practicable, disclose to the defense the existence of evidence that reasonably tends to impeach the credibility of a witness whom the government intends to call at trial.

(3) The trial counsel shall, as soon as practicable upon a finding of guilt, disclose to the defense the existence of evidence that is not subject to paragraph (1) or paragraph (2) but that reasonably may be viewed as mitigation evidence at sentencing.

(4) The disclosure obligations under this subsection encompass evidence that is known or reasonably should be known to any government officials who participated in the investigation and prosecution of the case against the defendant.

DEFENSE OF LACK OF MENTAL RESPONSIBILITY

SEC. 949K.

(a) AFFIRMATIVE DEFENSE.—It is an affirmative defense in a trial by military commission under this chapter that, at the time of the commission of the acts constituting the offense, the accused, as a result of a severe mental disease or defect, was unable to appreciate the nature and quality or the wrongfulness of the acts. Mental disease or defect does not otherwise constitute a defense.

(b) BURDEN OF PROOF.—The accused in a military commission under this chapter has the burden of proving the defense of lack of mental responsibility by clear and convincing evidence.

(c) FINDINGS FOLLOWING ASSERTION OF DEFENSE.—Whenever lack of mental responsibility of the accused with respect to an offense is properly at issue in a military commission under this chapter, the military judge shall instruct the members as to the defense of lack of mental responsibility under this section and shall charge the members to find the accused—

(1) guilty;

(2) not guilty; or

(3) subject to subsection (d), not guilty by reason of lack of mental responsibility.

(d) MAJORITY VOTE REQUIRED FOR FINDING.—The accused shall be found not guilty by reason of lack of mental responsibility under subsection (c)(3) only if a majority of the members present at the time the vote is taken determines that the defense of lack of mental responsibility has been established.

VOTING AND RULINGS

SEC. 949L.

(a) VOTE BY SECRET WRITTEN BALLOT.—Voting by members of a military commission under this chapter on the findings and on the sentence shall be by secret written ballot.

(b) RULINGS.—

(1) The military judge in a military commission under this chapter shall rule upon all questions of law, including the admissibility of evidence and all interlocutory questions arising during the proceedings.

(2) Any ruling made by the military judge upon a question of law or an interlocutory question (other than the factual issue of mental responsibility of the accused) is conclusive and constitutes the ruling of the military commission. However, a military judge may change such a ruling at any time during the trial.

(c) INSTRUCTIONS PRIOR TO VOTE.—Before a vote is taken of the findings of a military commission under this chapter, the military judge shall, in the presence of the accused and counsel, instruct the members as to the elements of the offense and charge the members—

(1) that the accused must be presumed to be innocent until the accused's guilt is established by legal and competent evidence beyond a reasonable doubt;

(2) that in the case being considered, if there is a reasonable doubt as to the guilt of the accused, the doubt must be resolved in favor of the accused and the accused must be acquitted;

(3) that, if there is reasonable doubt as to the degree of guilt, the finding must be in a lower degree as to which there is no reasonable doubt; and

(4) that the burden of proof to establish the guilt of the accused beyond a reasonable doubt is upon the United States.

NUMBER OF VOTES REQUIRED

SEC. 949M.

(a) **CONVICTION.**—No person may be convicted by a military commission under this chapter of any offense, except as provided in section 949i(b) of this title or by concurrence of two-thirds of the primary members present at the time the vote is taken.

(b) **SENTENCES.**—

(1) Except as provided in paragraphs (2) and (3), sentences shall be determined by a military commission by the concurrence of two-thirds of the primary members present at the time the vote is taken.

(2) No person may be sentenced to death by a military commission, except insofar as—

(A) the penalty of death has been expressly authorized under this chapter, chapter 47 of this title, or the law of war for an offense of which the accused has been found guilty;

(B) trial counsel expressly sought the penalty of death by filing an appropriate notice in advance of trial;

(C) the accused was convicted of the offense by the concurrence of all the primary members present at the time the vote is taken, or a guilty plea was accepted and not withdrawn prior to announcement of the sentence in accordance with section 949i(b) of this title; and

(D) all primary members present at the time the vote was taken on the sentence concurred in the sentence of death.

(3) No person may be sentenced to life imprisonment, or to confinement for more than 10 years, by a military commission under this chapter except by the concurrence of three-fourths of the primary members present at the time the vote is taken.

(4) The primary members present for a vote on a sentence need not be the same primary members who voted on the conviction if the requirements of section 948m(d) of this title are met.

(c) **NUMBER OF MEMBERS REQUIRED FOR PENALTY OF DEATH.**—

(1) Except as provided in paragraph (2), in a case in which the penalty of death is sought, the number of primary members of the military commission under this chapter shall be not less than 12 primary members.

(2) In any case described in paragraph (1) in which 12 primary members are not reasonably available for a military commission because of physical conditions or military exigencies, the convening authority shall specify a lesser number of primary members for the military commission

(but not fewer than 9 primary members), and the military commission may be assembled, and the trial held, with not less than the number of primary members so specified. In any such case, the convening authority shall make a detailed written statement, to be appended to the record, stating why a greater number of primary members were not reasonably available.

MILITARY COMMISSION TO ANNOUNCE ACTION

SEC. 949N.

A military commission under this chapter shall announce its findings and sentence to the parties as soon as determined.

RECORD OF TRIAL

SEC. 949O.

(a) **RECORD; AUTHENTICATION.**—Each military commission under this chapter shall keep a separate, verbatim, record of the proceedings in each case brought before it, and the record shall be authenticated by the signature of the military judge. If the record cannot be authenticated by the military judge by reason of death, disability, or absence, it shall be authenticated by the signature of the trial counsel or by a member of the commission if the trial counsel is unable to authenticate it by reason of death, disability, or absence. Where appropriate, and as provided in regulations prescribed by the Secretary of Defense, the record of a military commission under this chapter may contain a classified annex.

(b) **COMPLETE RECORD REQUIRED.**—A complete record of the proceedings and testimony shall be prepared in every military commission under this chapter.

(c) **PROVISION OF COPY TO ACCUSED.**—A copy of the record of the proceedings of the military commission under this chapter shall be given the accused as soon as it is authenticated. If the record contains classified information, or a classified annex, the accused shall receive a redacted version of the record consistent with the requirements of subchapter V of this chapter. Defense counsel shall have access to the unredacted record, as provided in regulations prescribed by the Secretary of Defense.

SUBCHAPTER V—CLASSIFIED INFORMATION PROCEDURES

**PROTECTION OF CLASSIFIED INFORMATION:
APPLICABILITY OF SUBCHAPTER**

SEC. 949P-1.

(a) **PROTECTION OF CLASSIFIED INFORMATION.**—Classified information shall be protected and is privileged from disclosure if disclosure would be detrimental to the national security. Under no circumstances may a military judge order the release of classified information to any person not authorized to receive such information.

(b) **ACCESS TO EVIDENCE.**—Any information admitted into evidence pursuant to any rule, procedure, or order by the military judge shall be provided to the accused.

(c) **DECLASSIFICATION.**—Trial counsel shall work with the original classification authorities for evidence that may be used at trial to ensure that such evidence is declassified to the maximum extent possible, consistent with the requirements of national security. A decision not to declassify evidence under this section shall not be subject to review by a military commission or upon appeal.

(d) **CONSTRUCTION OF PROVISIONS.**—The judicial construction of the Classified Information Procedures Act (18 U.S.C. App.) shall be authoritative in the interpretation of this subchapter, except to the extent that such construction is inconsistent with the specific requirements of this chapter.

PRETRIAL CONFERENCE

SEC. 949P-2.

(a) **MOTION.**—At any time after service of charges, any party may move for a pretrial conference to consider matters relating to classified information that may arise in connection with the prosecution.

(b) **CONFERENCE.**—Following a motion under subsection (a), or sua sponte, the military judge shall promptly hold a pretrial conference. Upon request by either party, the court shall hold such conference ex parte to the extent necessary to protect classified information from disclosure, in accordance with the practice of the Federal courts under the Classified Information Procedures Act (18 U.S.C. App.).

(c) **MATTERS TO BE ESTABLISHED AT PRETRIAL CONFERENCE.**—

(1) **TIMING OF SUBSEQUENT ACTIONS.**—At the pretrial conference, the military judge shall establish the timing of—

(A) requests for discovery;

(B) the provision of notice required by section 949p-5 of this title; and

(C) the initiation of the procedure established by section 949p-6 of this title.

(2) OTHER MATTERS.—At the pretrial conference, the military judge may also consider any matter—

(A) which relates to classified information; or

(B) which may promote a fair and expeditious trial.

(d) EFFECT OF ADMISSIONS BY ACCUSED AT PRETRIAL CONFERENCE.—No admission made by the accused or by any counsel for the accused at a pretrial conference under this section may be used against the accused unless the admission is in writing and is signed by the accused and by the counsel for the accused.

PROTECTIVE ORDERS

SEC. 949P-3.

Upon motion of the trial counsel, the military judge shall issue an order to protect against the disclosure of any classified information that has been disclosed by the United States to any accused in any military commission under this chapter or that has otherwise been provided to, or obtained by, any such accused in any such military commission.

DISCOVERY OF, AND ACCESS TO, CLASSIFIED INFORMATION BY THE ACCUSED

SEC. 949P-4.

(a) LIMITATIONS ON DISCOVERY OR ACCESS BY THE ACCUSED.—

(1) DECLARATIONS BY THE UNITED STATES OF DAMAGE TO NATIONAL SECURITY.—In any case before a military commission in which the United States seeks to delete, withhold, or otherwise obtain other relief with respect to the discovery of or access to any classified information, the trial counsel shall submit a declaration invoking the United States' classified information privilege and setting forth the damage to the national security that the discovery of or access to such information reasonably could be expected to cause. The declaration shall be signed by a knowledgeable United States official possessing authority to classify information.

(2) STANDARD FOR AUTHORIZATION OF DISCOVERY OR ACCESS.—Upon the submission of a declaration under paragraph (1), the military judge may not authorize the discovery of or access to such classified

information unless the military judge determines that such classified information would be noncumulative, relevant, and helpful to a legally cognizable defense, rebuttal of the prosecution's case, or to sentencing, in accordance with standards generally applicable to discovery of or access to classified information in Federal criminal cases. If the discovery of or access to such classified information is authorized, it shall be addressed in accordance with the requirements of subsection (b).

(b) DISCOVERY OF CLASSIFIED INFORMATION.—

(1) SUBSTITUTIONS AND OTHER RELIEF.—The military judge, in assessing the accused's discovery of or access to classified information under this section, may authorize the United States—

(A) to delete or withhold specified items of classified information;

(B) to substitute a summary for classified information; or

(C) to substitute a statement admitting relevant facts that the classified information or material would tend to prove.

(2) EX PARTE PRESENTATIONS.—The military judge shall permit the trial counsel to make a request for an authorization under paragraph (1) in the form of an ex parte presentation to the extent necessary to protect classified information, in accordance with the practice of the Federal courts under the Classified Information Procedures Act (18 U.S.C. App.). If the military judge enters an order granting relief following such an ex parte showing, the entire presentation (including the text of any written submission, verbatim transcript of the ex parte oral conference or hearing, and any exhibits received by the court as part of the ex parte presentation) shall be sealed and preserved in the records of the military commission to be made available to the appellate court in the event of an appeal.

(3) ACTION BY MILITARY JUDGE.—The military judge shall grant the request of the trial counsel to substitute a summary or to substitute a statement admitting relevant facts, or to provide other relief in accordance with paragraph (1), if the military judge finds that the summary, statement, or other relief would provide the accused with substantially the same ability to make a defense as would discovery of or access to the specific classified information.

(c) RECONSIDERATION.—An order of a military judge authorizing a request of the trial counsel to substitute, summarize, withhold, or prevent access to classified information under this section is not subject to a motion for reconsideration by the accused, if such order was entered pursuant to an ex parte showing under this section.

**NOTICE BY ACCUSED OF INTENTION TO DISCLOSE
CLASSIFIED INFORMATION**

SEC. 949P-5.

(a) NOTICE BY ACCUSED.—

(1) NOTIFICATION OF TRIAL COUNSEL AND MILITARY JUDGE.—If an accused reasonably expects to disclose, or to cause the disclosure of, classified information in any manner in connection with any trial or pretrial proceeding involving the prosecution of such accused, the accused shall, within the time specified by the military judge or, where no time is specified, within 30 days before trial, notify the trial counsel and the military judge in writing. Such notice shall include a brief description of the classified information. Whenever the accused learns of additional classified information the accused reasonably expects to disclose, or to cause the disclosure of, at any such proceeding, the accused shall notify trial counsel and the military judge in writing as soon as possible thereafter and shall include a brief description of the classified information.

(2) LIMITATION ON DISCLOSURE BY ACCUSED.—No accused shall disclose, or cause the disclosure of, any information known or believed to be classified in connection with a trial or pretrial proceeding until—

(A) notice has been given under paragraph (1); and

(B) the United States has been afforded a reasonable opportunity to seek a determination pursuant to the procedure set forth in section 949p-6 of this title and the time for the United States to appeal such determination under section 950d of this title has expired or any appeal under that section by the United States is decided.

(b) FAILURE TO COMPLY.—If the accused fails to comply with the requirements of subsection (a), the military judge—

(1) may preclude disclosure of any classified information not made the subject of notification; and

(2) may prohibit the examination by the accused of any witness with respect to any such information.

PROCEDURE FOR CASES INVOLVING CLASSIFIED INFORMATION

SEC. 949P-6.

(a) MOTION FOR HEARING.—

(1) REQUEST FOR HEARING.—Within the time specified by the military judge for the filing of a motion under this section, either party may

request the military judge to conduct a hearing to make all determinations concerning the use, relevance, or admissibility of classified information that would otherwise be made during the trial or pretrial proceeding.

(2) CONDUCT OF HEARING.—Upon a request by either party under paragraph (1), the military judge shall conduct such a hearing and shall rule prior to conducting any further proceedings.

(3) IN CAMERA HEARING UPON DECLARATION TO COURT BY APPROPRIATE OFFICIAL OF RISK OF DISCLOSURE OF CLASSIFIED INFORMATION.—Any hearing held pursuant to this subsection (or any portion of such hearing specified in the request of a knowledgeable United States official) shall be held in camera if a knowledgeable United States official possessing authority to classify information submits to the military judge a declaration that a public proceeding may result in the disclosure of classified information. Classified information is not subject to disclosure under this section unless the information is relevant and necessary to an element of the offense or a legally cognizable defense and is otherwise admissible in evidence.

(4) MILITARY JUDGE TO MAKE DETERMINATIONS IN WRITING.—As to each item of classified information, the military judge shall set forth in writing the basis for the determination.

(b) NOTICE AND USE OF CLASSIFIED INFORMATION BY THE GOVERNMENT.—

(1) NOTICE TO ACCUSED.—Before any hearing is conducted pursuant to a request by the trial counsel under subsection (a), trial counsel shall provide the accused with notice of the classified information that is at issue. Such notice shall identify the specific classified information at issue whenever that information previously has been made available to the accused by the United States. When the United States has not previously made the information available to the accused in connection with the case the information may be described by generic category, in such forms as the military judge may approve, rather than by identification of the specific information of concern to the United States.

(2) ORDER BY MILITARY JUDGE UPON REQUEST OF ACCUSED.—

Whenever the trial counsel requests a hearing under subsection (a), the military judge, upon request of the accused, may order the trial counsel to provide the accused, prior to trial, such details as to the portion of the charge or specification at issue in the hearing as are needed to give the accused fair notice to prepare for the hearing.

(c) SUBSTITUTIONS.—

(1) IN CAMERA PRETRIAL HEARING.—Upon request of the trial counsel pursuant to the Military Commission Rules of Evidence, and in

accordance with the security procedures established by the military judge, the military judge shall conduct a classified in camera pretrial hearing concerning the admissibility of classified information.

(2) PROTECTION OF SOURCES, METHODS, AND ACTIVITIES BY WHICH EVIDENCE ACQUIRED.—When trial counsel seeks to introduce evidence before a military commission under this chapter and the Executive branch has classified the sources, methods, or activities by which the United States acquired the evidence, the military judge shall permit trial counsel to introduce the evidence, including a substituted evidentiary foundation pursuant to the procedures described in subsection (d), while protecting from disclosure information identifying those sources, methods, or activities, if—

(A) the evidence is otherwise admissible; and

(B) the military judge finds that—

(i) the evidence is reliable; and

(ii) the redaction is consistent with affording the accused a fair trial.

(d) ALTERNATIVE PROCEDURE FOR DISCLOSURE OF CLASSIFIED INFORMATION.—

(1) MOTION BY THE UNITED STATES.—Upon any determination by the military judge authorizing the disclosure of specific classified information under the procedures established by this section, the trial counsel may move that, in lieu of the disclosure of such specific classified information, the military judge order—

(A) the substitution for such classified information of a statement admitting relevant facts that the specific classified information would tend to prove;

(B) the substitution for such classified information of a summary of the specific classified information; or

(C) any other procedure or redaction limiting the disclosure of specific classified information.

(2) ACTION ON MOTION.—The military judge shall grant such a motion of the trial counsel if the military judge finds that the statement, summary, or other procedure or redaction will provide the defendant with substantially the same ability to make his defense as would disclosure of the specific classified information.

(3) HEARING ON MOTION.—The military judge shall hold a hearing on any motion under this subsection. Any such hearing shall be held in camera at the request of a knowledgeable United States official possessing authority to classify information.

(4) SUBMISSION OF STATEMENT OF DAMAGE TO NATIONAL SECURITY IF DISCLOSURE ORDERED.—The trial counsel may, in connection with a motion under paragraph (1), submit to the military judge a declaration signed by a knowledgeable United States official possessing authority to classify information certifying that disclosure of classified information would cause identifiable damage to the national security of the United States and explaining the basis for the classification of such information. If so requested by the trial counsel, the military judge shall examine such declaration during an ex parte presentation.

(e) SEALING OF RECORDS OF IN CAMERA HEARINGS.—If at the close of an in camera hearing under this section (or any portion of a hearing under this section that is held in camera), the military judge determines that the classified information at issue may not be disclosed or elicited at the trial or pretrial proceeding, the record of such in camera hearing shall be sealed and preserved for use in the event of an appeal. The accused may seek reconsideration of the military judge's determination prior to or during trial.

(f) PROHIBITION ON DISCLOSURE OF CLASSIFIED INFORMATION BY THE ACCUSED; RELIEF FOR ACCUSED WHEN THE UNITED STATES OPPOSES DISCLOSURE.—

(1) ORDER TO PREVENT DISCLOSURE BY ACCUSED.—Whenever the military judge denies a motion by the trial counsel that the judge issue an order under subsection (a), (c), or (d) and the trial counsel files with the military judge a declaration signed by a knowledgeable United States official possessing authority to classify information objecting to disclosure of the classified information at issue, the military judge shall order that the accused not disclose or cause the disclosure of such information.

(2) RESULT OF ORDER UNDER PARAGRAPH (1).—Whenever an accused is prevented by an order under paragraph (1) from disclosing or causing the disclosure of classified information, the military judge shall dismiss the case, except that, when the military judge determines that the interests of justice would not be served by dismissal of the case, the military judge shall order such other action, in lieu of dismissing the charge or specification, as the military judge determines is appropriate. Such action may include, but need not be limited to, the following:

(A) Dismissing specified charges or specifications.

(B) Finding against the United States on any issue as to which the excluded classified information relates.

(C) Striking or precluding all or part of the testimony of a witness.

(3) TIME FOR THE UNITED STATES TO SEEK INTERLOCUTORY APPEAL.—An order under paragraph (2) shall not take effect until the military judge has afforded the United States—

(A) an opportunity to appeal such order under section 950d of this title; and

(B) an opportunity thereafter to withdraw its objection to the disclosure of the classified information at issue.

(g) RECIPROCIITY.—

(1) DISCLOSURE OF REBUTTAL INFORMATION.—Whenever the military judge determines that classified information may be disclosed in connection with a trial or pretrial proceeding, the military judge shall, unless the interests of fairness do not so require, order the United States to provide the accused with the information it expects to use to rebut the classified information. The military judge may place the United States under a continuing duty to disclose such rebuttal information.

(2) SANCTION FOR FAILURE TO COMPLY.—If the United States fails to comply with its obligation under this subsection, the military judge—

(A) may exclude any evidence not made the subject of a required disclosure; and

(B) may prohibit the examination by the United States of any witness with respect to such information.

INTRODUCTION OF CLASSIFIED INFORMATION INTO EVIDENCE

SEC. 949P-7.

(a) PRESERVATION OF CLASSIFICATION STATUS.—Writings, recordings, and photographs containing classified information may be admitted into evidence in proceedings of military commissions under this chapter without change in their classification status.

(b) PRECAUTIONS BY MILITARY JUDGES.—

(1) PRECAUTIONS IN ADMITTING CLASSIFIED INFORMATION INTO EVIDENCE.—The military judge in a trial by military commission, in order to prevent unnecessary disclosure of classified information, may order admission into evidence of only part of a writing, recording, or photograph, or may order admission into evidence of the whole writing, recording, or photograph with excision of some or all of the classified information contained therein, unless the whole ought in fairness be considered.

(2) CLASSIFIED INFORMATION KEPT UNDER SEAL.—The military judge shall allow classified information offered or accepted into evidence to remain under seal during the trial, even if such evidence is disclosed in

the military commission, and may, upon motion by the United States, seal exhibits containing classified information for any period after trial as necessary to prevent a disclosure of classified information when a knowledgeable United States official possessing authority to classify information submits to the military judge a declaration setting forth the damage to the national security that the disclosure of such information reasonably could be expected to cause.

(c) TAKING OF TESTIMONY.—

(1) OBJECTION BY TRIAL COUNSEL.—During the examination of a witness, trial counsel may object to any question or line of inquiry that may require the witness to disclose classified information not previously found to be admissible.

(2) ACTION BY MILITARY JUDGE.—Following an objection under paragraph (1), the military judge shall take such suitable action to determine whether the response is admissible as will safeguard against the compromise of any classified information. Such action may include requiring trial counsel to provide the military judge with a proffer of the witness' response to the question or line of inquiry and requiring the accused to provide the military judge with a proffer of the nature of the information sought to be elicited by the accused. Upon request, the military judge may accept an ex parte proffer by trial counsel to the extent necessary to protect classified information from disclosure, in accordance with the practice of the Federal courts under the Classified Information Procedures Act (18 U.S.C. App.).

(d) DISCLOSURE AT TRIAL OF CERTAIN STATEMENTS PREVIOUSLY MADE BY A WITNESS.—

(1) MOTION FOR PRODUCTION OF STATEMENTS IN POSSESSION OF THE UNITED STATES.—After a witness called by the trial counsel has testified on direct examination, the military judge, on motion of the accused, may order production of statements of the witness in the possession of the United States which relate to the subject matter as to which the witness has testified. This paragraph does not preclude discovery or assertion of a privilege otherwise authorized.

(2) INVOCATION OF PRIVILEGE BY THE UNITED STATES.—If the United States invokes a privilege, the trial counsel may provide the prior statements of the witness to the military judge during an ex parte presentation to the extent necessary to protect classified information from disclosure, in accordance with the practice of the Federal courts under the Classified Information Procedures Act (18 U.S.C. App.).

(3) ACTION BY MILITARY JUDGE ON MOTION.—If the military judge finds that disclosure of any portion of the statement identified by the

United States as classified would be detrimental to the national security in the degree to warrant classification under the applicable Executive Order, statute, or regulation, that such portion of the statement is consistent with the testimony of the witness, and that the disclosure of such portion is not necessary to afford the accused a fair trial, the military judge shall excise that portion from the statement. If the military judge finds that such portion of the statement is inconsistent with the testimony of the witness or that its disclosure is necessary to afford the accused a fair trial, the military judge, shall, upon the request of the trial counsel, review alternatives to disclosure in accordance with section 949p-6(d) of this title.

SUBCHAPTER VI—SENTENCES

CRUEL OR UNUSUAL PUNISHMENTS PROHIBITED

SEC. 949S.

Punishment by flogging, or by branding, marking, or tattooing on the body, or any other cruel or unusual punishment, may not be adjudged by a military commission under this chapter or inflicted under this chapter upon any person subject to this chapter. The use of irons, single or double, except for the purpose of safe custody, is prohibited under this chapter.

MAXIMUM LIMITS

SEC. 949T.

The punishment which a military commission under this chapter may direct for an offense may not exceed such limits as the President or Secretary of Defense may prescribe for that offense.

EXECUTION OF CONFINEMENT

SEC. 949U.

(a) **IN GENERAL.**—Under such regulations as the Secretary of Defense may prescribe, a sentence of confinement adjudged by a military commission under this chapter may be carried into execution by confinement—

- (1) in any place of confinement under the control of any of the armed forces; or
- (2) in any penal or correctional institution under the control of the United States or its allies, or which the United States may be allowed to use.

(b) **TREATMENT DURING CONFINEMENT BY OTHER THAN THE ARMED**

FORCES.—Persons confined under subsection (a)(2) in a penal or correctional

institution not under the control of an armed force are subject to the same discipline and treatment as persons confined or committed by the courts of the United States or of the State, District of Columbia, or place in which the institution is situated.

SUBCHAPTER VII—POST-TRIAL PROCEDURE AND REVIEW OF MILITARY COMMISSIONS

ERROR OF LAW; LESSER INCLUDED OFFENSE

SEC. 950A.

(a) **ERROR OF LAW.**—A finding or sentence of a military commission under this chapter may not be held incorrect on the ground of an error of law unless the error materially prejudices the substantial rights of the accused.

(b) **LESSER INCLUDED OFFENSE.**—Any reviewing authority with the power to approve or affirm a finding of guilty by a military commission under this chapter may approve or affirm, instead, so much of the finding as includes a lesser included offense.

REVIEW BY THE CONVENING AUTHORITY

SEC. 950B.

(a) **NOTICE TO CONVENING AUTHORITY OF FINDINGS AND SENTENCE.**—The findings and sentence of a military commission under this chapter shall be reported in writing promptly to the convening authority after the announcement of the sentence.

(b) **SUBMITTAL OF MATTERS BY ACCUSED TO CONVENING AUTHORITY.**—(1) The accused may submit to the convening authority matters for consideration by the convening authority with respect to the findings and the sentence of the military commission under this chapter.

(2)(A) Except as provided in subparagraph (B), a submittal under paragraph (1) shall be made in writing within 20 days after the accused has been given an authenticated record of trial under section 949o(c) of this title.

(B) If the accused shows that additional time is required for the accused to make a submittal under paragraph (1), the convening authority may, for good cause, extend the applicable period under subparagraph (A) for not more than an additional 20 days.

(3) The accused may waive the accused's right to make a submittal to the convening authority under paragraph (1). Such a waiver shall be made in writing, and may not be revoked. For the purposes of subsection (c)(2),

the time within which the accused may make a submittal under this subsection shall be deemed to have expired upon the submittal of a waiver under this paragraph to the convening authority.

(c) ACTION BY CONVENING AUTHORITY.—

(1) The authority under this subsection to modify the findings and sentence of a military commission under this chapter is a matter of the sole discretion and prerogative of the convening authority.

(2) The convening authority is not required to take action on the findings of a military commission under this chapter. If the convening authority takes action on the findings, the convening authority may, in the sole discretion of the convening authority, only—

(A) dismiss any charge or specification by setting aside a finding of guilty thereto; or

(B) change a finding of guilty to a charge to a finding of guilty to an offense that is a lesser included offense of the offense stated in the charge.

(3)(A) The convening authority shall take action on the sentence of a military commission under this chapter.

(B) Subject to regulations prescribed by the Secretary of Defense, action under this paragraph may be taken only after consideration of any matters submitted by the accused under subsection (b) or after the time for submitting such matters expires, whichever is earlier.

(C) In taking action under this paragraph, the convening authority may, in the sole discretion of the convening authority, approve, disapprove, commute, or suspend the sentence in whole or in part. The convening authority may not increase a sentence beyond that which is found by the military commission.

(4) The convening authority shall serve on the accused or on defense counsel notice of any action taken by the convening authority under this subsection.

(d) ORDER OF REVISION OR REHEARING.—

(1) Subject to paragraphs (2) and (3), the convening authority of a military commission under this chapter may, in the sole discretion of the convening authority, order a proceeding in revision or a rehearing.

(2)(A) Except as provided in subparagraph (B), a proceeding in revision may be ordered by the convening authority if—

(i) there is an apparent error or omission in the record; or

(ii) the record shows improper or inconsistent action by the military commission with respect to the findings or

sentence that can be rectified without material prejudice to the substantial rights of the accused.

(B) In no case may a proceeding in revision—

(i) reconsider a finding of not guilty of a specification or a ruling which amounts to a finding of not guilty;

(ii) reconsider a finding of not guilty of any charge, unless there has been a finding of guilty under a specification laid under that charge, which sufficiently alleges a violation; or

(iii) increase the severity of the sentence unless the sentence prescribed for the offense is mandatory.

(3) A rehearing may be ordered by the convening authority if the convening authority disapproves the findings and sentence and states the reasons for disapproval of the findings. If the convening authority disapproves the finding and sentence and does not order a rehearing, the convening authority shall dismiss the charges. A rehearing as to the findings may not be ordered by the convening authority when there is a lack of sufficient evidence in the record to support the findings. A rehearing as to the sentence may be ordered by the convening authority if the convening authority disapproves the sentence.

APPELLATE REFERRAL; WAIVER OR WITHDRAWAL OF APPEAL

SEC. 950C.

(a) **AUTOMATIC REFERRAL FOR APPELLATE REVIEW.**—Except as provided in subsection (b), in each case in which the final decision of a military commission under this chapter (as approved by the convening authority) includes a finding of guilty, the convening authority shall refer the case to the United States Court of Military Commission Review. Any such referral shall be made in accordance with procedures prescribed under regulations of the Secretary.

(b) **WAIVER OF RIGHT OF REVIEW.**—

(1) Except in a case in which the sentence as approved under section 950b of this title extends to death, an accused may file with the convening authority a statement expressly waiving the right of the accused to appellate review by the United States Court of Military Commission Review under section 950f of this title of the final decision of the military commission under this chapter.

(2) A waiver under paragraph (1) shall be signed by both the accused and a defense counsel.

(3) A waiver under paragraph (1) must be filed, if at all, within 10 days after notice of the action is served on the accused or on defense counsel

under section 950b(c)(4) of this title. The convening authority, for good cause, may extend the period for such filing by not more than 30 days.

(c) **WITHDRAWAL OF APPEAL.**—Except in a case in which the sentence as approved under section 950b of this title extends to death, the accused may withdraw an appeal at any time.

(d) **EFFECT OF WAIVER OR WITHDRAWAL.**—A waiver of the right to appellate review or the withdrawal of an appeal under this section bars review under section 950f of this title.

INTERLOCUTORY APPEALS BY THE UNITED STATES

SEC. 950D.

(a) **INTERLOCUTORY APPEAL.**—Except as provided in subsection (b), in a trial by military commission under this chapter, the United States may take an interlocutory appeal to the United States Court of Military Commission Review of any order or ruling of the military judge—

- (1) that terminates proceedings of the military commission with respect to a charge or specification;
- (2) that excludes evidence that is substantial proof of a fact material in the proceeding;
- (3) that relates to a matter under subsection (c) or (d) of section 949d of this title; or
- (4) that, with respect to classified information—
 - (A) authorizes the disclosure of such information;
 - (B) imposes sanctions for nondisclosure of such information; or
 - (C) refuses a protective order sought by the United States to prevent the disclosure of such information.

(b) **LIMITATION.**—The United States may not appeal under subsection (a) an order or ruling that is, or amounts to, a finding of not guilty by the military commission with respect to a charge or specification.

(c) **SCOPE OF APPEAL RIGHT WITH RESPECT TO CLASSIFIED INFORMATION.**—The United States has the right to appeal under paragraph (4) of subsection (a) whenever the military judge enters an order or ruling that would require the disclosure of classified information, without regard to whether the order or ruling appealed from was entered under this chapter, another provision of law, a rule, or otherwise. Any such appeal may embrace any preceding order, ruling, or reasoning constituting the basis of the order or ruling that would authorize such disclosure.

(d) **TIMING AND ACTION ON INTERLOCUTORY APPEALS RELATING TO CLASSIFIED INFORMATION.**—

TITLE 10, MILITARY COMMISSIONS

(1) **APPEAL TO BE EXPEDITED.**—An appeal taken pursuant to paragraph (4) of subsection (a) shall be expedited by the United States Court of Military Commission Review.

(2) **APPEALS BEFORE TRIAL.**—If such an appeal is taken before trial, the appeal shall be taken within 10 days after the order or ruling from which the appeal is made and the trial shall not commence until the appeal is decided.

(3) **APPEALS DURING TRIAL.**—If such an appeal is taken during trial, the military judge shall adjourn the trial until the appeal is decided, and the court of appeals—

(A) shall hear argument on such appeal within 4 days of the adjournment of the trial (excluding weekends and holidays);

(B) may dispense with written briefs other than the supporting materials previously submitted to the military judge;

(C) shall render its decision within four days of argument on appeal (excluding weekends and holidays); and

(D) may dispense with the issuance of a written opinion in rendering its decision.

(e) **NOTICE AND TIMING OF OTHER APPEALS.**—The United States shall take an appeal of an order or ruling under subsection (a), other than an appeal under paragraph (4) of that subsection, by filing a notice of appeal with the military judge within 5 days after the date of the order or ruling.

(f) **METHOD OF APPEAL.**—An appeal under this section shall be forwarded, by means specified in regulations prescribed by the Secretary of Defense, directly to the United States Court of Military Commission Review.

(g) **APPEALS COURT TO ACT ONLY WITH RESPECT TO MATTER OF LAW.**—In ruling on an appeal under paragraph (1), (2), or (3) of subsection (a), the appeals court may act only with respect to matters of law.

(h) **SUBSEQUENT APPEAL RIGHTS OF ACCUSED NOT AFFECTED.**—An appeal under paragraph (4) of subsection (a), and a decision on such appeal, shall not affect the right of the accused, in a subsequent appeal from a judgment of conviction, to claim as error reversal by the military judge on remand of a ruling appealed from during trial.

REHEARINGS

SEC. 950E.

(a) **COMPOSITION OF MILITARY COMMISSION FOR REHEARING.**—Each rehearing under this chapter shall take place before a military commission under this chapter composed of members who were not members of the military commission which first heard the case.

(b) SCOPE OF REHEARING.—

(1) Upon a rehearing—

(A) the accused may not be tried for any offense of which the accused was found not guilty by the first military commission; and

(B) no sentence in excess of or more than the original sentence may be imposed unless—

(i) the sentence is based upon a finding of guilty of an offense not considered upon the merits in the original proceedings; or

(ii) the sentence prescribed for the offense is mandatory.

(2) Upon a rehearing, if the sentence approved after the first military commission was in accordance with a pretrial agreement and the accused at the rehearing changes his plea with respect to the charges or specifications upon which the pretrial agreement was based, or otherwise does not comply with pretrial agreement, the sentence as to those charges or specifications may include any punishment not in excess of that lawfully adjudged at the first military commission.

REVIEW BY UNITED STATES COURT OF MILITARY COMMISSION REVIEW

SEC. 950F.

(a) ESTABLISHMENT.—There is a court of record to be known as the “United States Court of Military Commission Review” (in this section referred to as the “Court”). The Court shall consist of one or more panels, each composed of not less than three judges on the Court. For the purpose of reviewing decisions of military commissions under this chapter, the Court may sit in panels or as a whole, in accordance with rules prescribed by the Secretary of Defense.

(b) JUDGES.—

(1) Judges on the Court shall be assigned or appointed in a manner consistent with the provisions of this subsection.

(2) The Secretary of Defense may assign persons who are appellate military judges to be judges on the Court. Any judge so assigned shall be a commissioned officer of the armed forces, and shall meet the qualifications for military judges prescribed by section 948j(b) of this title.

(3) The President may appoint, by and with the advice and consent of the Senate, additional judges to the United States Court of Military Commission Review.

(4) No person may serve as a judge on the Court in any case in which that person acted as a military judge, counsel, or reviewing official.

(5)(A) For purposes of sections 203, 205, 207, 208, and 209 of title 18, the term “special Government employee” shall include a judge of the Court appointed under paragraph (3).

(B) A person appointed as a judge of the Court under paragraph (3) shall be considered to be an officer or employee of the United States with respect to such person’s status as a judge, but only during periods in which such person is performing the duties of such a judge. Any provision of law that prohibits or limits the political or business activities of an employee of the United States shall only apply to such a judge during such periods.

(6) The term of an appellate military judge assigned to the Court under paragraph (2) or appointed to the Court under paragraph (3) shall expire on the earlier of the date on which—

(A) the judge leaves active duty; or

(B) the judge is reassigned to other duties in accordance with section 949b(b)(4) of this title.

(c) CASES TO BE REVIEWED.—The Court shall, in accordance with procedures prescribed under regulations of the Secretary, review the record in each case that is referred to the Court by the convening authority under section 950c of this title with respect to any matter properly raised by the accused.

(d) STANDARD AND SCOPE OF REVIEW.—In a case reviewed by the Court under this section, the Court may act only with respect to the findings and sentence as approved by the convening authority. The Court may affirm only such findings of guilty, and the sentence or such part or amount of the sentence, as the Court finds correct in law and fact and determines, on the basis of the entire record, should be approved. In considering the record, the Court may weigh the evidence, judge the credibility of witnesses, and determine controverted questions of fact, recognizing that the military commission saw and heard the witnesses.

(e) REHEARINGS.—If the Court sets aside the findings or sentence, the Court may, except where the setting aside is based on lack of sufficient evidence in the record to support the findings, order a rehearing. If the Court sets aside the findings or sentence and does not order a rehearing, the Court shall order that the charges be dismissed.

REVIEW BY UNITED STATES COURT OF APPEALS FOR THE DISTRICT OF COLUMBIA CIRCUIT; WRIT OF CERTIORARI TO SUPREME COURT

SEC. 950G.

(a) EXCLUSIVE APPELLATE JURISDICTION.—Except as provided in subsection (b), the United States Court of Appeals for the District of Columbia Circuit shall

have exclusive jurisdiction to determine the validity of a final judgment rendered by a military commission (as approved by the convening authority and, where applicable, as affirmed or set aside as incorrect in law by the United States Court of Military Commission Review) under this chapter.

(b) EXHAUSTION OF OTHER APPEALS.—The United States Court of Appeals for the District of Columbia Circuit may not review a final judgment described in subsection (a) until all other appeals under this chapter have been waived or exhausted.

(c) TIME FOR SEEKING REVIEW.—A petition for review by the United States Court of Appeals for the District of Columbia Circuit must be filed in the Court of Appeals—

(1) not later than 20 days after the date on which written notice of the final decision of the United States Court of Military Commission Review is served on the parties; or

(2) if the accused submits, in the form prescribed by section 950c of this title, a written notice waiving the right of the accused to review by the United States Court of Military Commission Review, not later than 20 days after the date on which such notice is submitted.

(d) SCOPE AND NATURE OF REVIEW.—The United States Court of Appeals for the District of Columbia Circuit may act under this section only with respect to the findings and sentence as approved by the convening authority and as affirmed or set aside as incorrect in law by the United States Court of Military Commission Review, and shall take action only with respect to matters of law, including the sufficiency of the evidence to support the verdict.

(e) REVIEW BY SUPREME COURT.—The Supreme Court may review by writ of certiorari pursuant to section 1254 of title 28 the final judgment of the United States Court of Appeals for the District of Columbia Circuit under this section.

APPELLATE COUNSEL

SEC. 950H.

(a) APPOINTMENT.—The Secretary of Defense shall, by regulation, establish procedures for the appointment of appellate counsel for the United States and for the accused in military commissions under this chapter. Appellate counsel shall meet the qualifications of counsel for appearing before military commissions under this chapter.

(b) REPRESENTATION OF UNITED STATES.—Appellate counsel appointed under subsection (a)—

(1) shall represent the United States in any appeal or review proceeding under this chapter before the United States Court of Military Commission Review; and

(2) may, when requested to do so by the Attorney General in a case arising under this chapter, represent the United States before the United States Court of Appeals for the District of Columbia Circuit or the Supreme Court.

(c) REPRESENTATION OF ACCUSED.—The accused shall be represented by appellate counsel appointed under subsection (a) before the United States Court of Military Commission Review, the United States Court of Appeals for the District of Columbia Circuit, and the Supreme Court, and by civilian counsel if retained by the accused. Any such civilian counsel shall meet the qualifications under paragraph (3) of section 949c(b) of this title for civilian counsel appearing before military commissions under this chapter and shall be subject to the requirements of paragraph (7) of that section.

EXECUTION OF SENTENCE; SUSPENSION OF SENTENCE

SEC. 950I.

(a) IN GENERAL.—The Secretary of Defense is authorized to carry out a sentence imposed by a military commission under this chapter in accordance with such procedures as the Secretary may prescribe.

(b) EXECUTION OF SENTENCE OF DEATH ONLY UPON APPROVAL BY THE PRESIDENT.—If the sentence of a military commission under this chapter extends to death, that part of the sentence providing for death may not be executed until approved by the President. In such a case, the President may commute, remit, or suspend the sentence, or any part thereof, as he sees fit.

(c) EXECUTION OF SENTENCE OF DEATH ONLY UPON FINAL JUDGMENT OF LEGALITY OF PROCEEDINGS.—

(1) If the sentence of a military commission under this chapter extends to death, the sentence may not be executed until there is a final judgment as to the legality of the proceedings (and with respect to death, approval under subsection (b)).

(2) A judgment as to legality of proceedings is final for purposes of paragraph (1) when review is completed in accordance with the judgment of the United States Court of Military Commission Review and—

(A) the time for the accused to file a petition for review by the United States Court of Appeals for the District of Columbia Circuit has expired, the accused has not filed a timely petition for such review, and the case is not otherwise under review by the Court of Appeals; or

(B) review is completed in accordance with the judgment of the United States Court of Appeals for the District of Columbia Circuit and—

- (i) a petition for a writ of certiorari is not timely filed;
- (ii) such a petition is denied by the Supreme Court; or
- (iii) review is otherwise completed in accordance with the judgment of the Supreme Court.

(d) **SUSPENSION OF SENTENCE.**—The Secretary of the Defense, or the convening authority acting on the case (if other than the Secretary), may suspend the execution of any sentence or part thereof in the case, except a sentence of death.

FINALITY OF PROCEEDINGS, FINDINGS, AND SENTENCES

SEC. 950J.

The appellate review of records of trial provided by this chapter, and the proceedings, findings, and sentences of military commissions as approved, reviewed, or affirmed as required by this chapter, are final and conclusive. Orders publishing the proceedings of military commissions under this chapter are binding upon all departments, courts, agencies, and officers of the United States, subject only to action by the Secretary or the convening authority as provided in section 950i(c) of this title and the authority of the President.

SUBCHAPTER VIII—PUNITIVE MATTERS

DEFINITIONS; CONSTRUCTION OF CERTAIN OFFENSES; COMMON CIRCUMSTANCES

SEC. 950P.

(a) **DEFINITIONS.**—In this subchapter:

- (1) The term “military objective” means combatants and those objects during hostilities which, by their nature, location, purpose, or use, effectively contribute to the war-fighting or war-sustaining capability of an opposing force and whose total or partial destruction, capture, or neutralization would constitute a definite military advantage to the attacker under the circumstances at the time of an attack.
- (2) The term “protected person” means any person entitled to protection under one or more of the Geneva Conventions, including civilians not taking an active part in hostilities, military personnel placed out of combat by sickness, wounds, or detention, and military medical or religious personnel.
- (3) The term “protected property” means any property specifically protected by the law of war, including buildings dedicated to religion, education, art, science, or charitable purposes, historic monuments, hospitals, and places where the sick and wounded are collected, but only

if and to the extent such property is not being used for military purposes or is not otherwise a military objective. The term includes objects properly identified by one of the distinctive emblems of the Geneva Conventions, but does not include civilian property that is a military objective.

(b) **CONSTRUCTION OF CERTAIN OFFENSES.**—The intent required for offenses under paragraphs (1), (2), (3), (4), and (12) of section 950t of this title precludes the applicability of such offenses with regard to collateral damage or to death, damage, or injury incident to a lawful attack.

(c) **COMMON CIRCUMSTANCES.**—An offense specified in this subchapter is triable by military commission under this chapter only if the offense is committed in the context of and associated with hostilities.

(d) **EFFECT.**—The provisions of this subchapter codify offenses that have traditionally been triable by military commission. This chapter does not establish new crimes that did not exist before the date of the enactment of this subchapter, as amended by the National Defense Authorization Act for Fiscal Year 2010, but rather codifies those crimes for trial by military commission. Because the provisions of this subchapter codify offenses that have traditionally been triable under the law of war or otherwise triable by military commission, this subchapter does not preclude trial for offenses that occurred before the date of the enactment of this subchapter, as so amended.

PRINCIPALS

SEC. 950Q.

Any person punishable under this chapter who—

(1) commits an offense punishable by this chapter, or aids, abets, counsels, commands, or procures its commission;

(2) causes an act to be done which if directly performed by him would be punishable by this chapter; or

(3) is a superior commander who, with regard to acts punishable by this chapter, knew, had reason to know, or should have known, that a subordinate was about to commit such acts or had done so and who failed to take the necessary and reasonable measures to prevent such acts or to punish the perpetrators thereof, is a principal.

ACCESSORY AFTER THE FACT

SEC. 950R.

Any person subject to this chapter who, knowing that an offense punishable by this chapter has been committed, receives, comforts, or assists the offender in order to hinder or prevent his apprehension, trial, or punishment shall be punished as a military commission under this chapter may direct.

CONVICTION OF LESSER OFFENSES

SEC. 950S.

An accused may be found guilty of an offense necessarily included in the offense charged or of an attempt to commit either the offense charged or an attempt to commit either the offense charged or an offense necessarily included therein.

CRIMES TRIABLE BY MILITARY COMMISSION

SEC. 950T.

The following offenses shall be triable by military commission under this chapter at any time without limitation:

- (1) **MURDER OF PROTECTED PERSONS.**—Any person subject to this chapter who intentionally kills one or more protected persons shall be punished by death or such other punishment as a military commission under this chapter may direct.
- (2) **ATTACKING CIVILIANS.**—Any person subject to this chapter who intentionally engages in an attack upon a civilian population as such, or individual civilians not taking active part in hostilities, shall be punished, if death results to one or more of the victims, by death or such other punishment as a military commission under this chapter may direct, and, if death does not result to any of the victims, by such punishment, other than death, as a military commission under this chapter may direct.
- (3) **ATTACKING CIVILIAN OBJECTS.**—Any person subject to this chapter who intentionally engages in an attack upon a civilian object that is not a military objective shall be punished as a military commission under this chapter may direct.
- (4) **ATTACKING PROTECTED PROPERTY.**—Any person subject to this chapter who intentionally engages in an attack upon protected property shall be punished as a military commission under this chapter may direct.
- (5) **PILLAGING.**—Any person subject to this chapter who intentionally and in the absence of military necessity appropriates or seizes property for private or personal use, without the consent of a person with authority to permit such

appropriation or seizure, shall be punished as a military commission under this chapter may direct.

(6) DENYING QUARTER.—Any person subject to this chapter who, with effective command or control over subordinate groups, declares, orders, or otherwise indicates to those groups that there shall be no survivors or surrender accepted, with the intent to threaten an adversary or to conduct hostilities such that there would be no survivors or surrender accepted, shall be punished as a military commission under this chapter may direct.

(7) TAKING HOSTAGES.—Any person subject to this chapter who, having knowingly seized or detained one or more persons, threatens to kill, injure, or continue to detain such person or persons with the intent of compelling any nation, person other than the hostage, or group of persons to act or refrain from acting as an explicit or implicit condition for the safety or release of such person or persons, shall be punished, if death results to one or more of the victims, by death or such other punishment as a military commission under this chapter may direct, and, if death does not result to any of the victims, by such punishment, other than death, as a military commission under this chapter may direct.

(8) EMPLOYING POISON OR SIMILAR WEAPONS.—Any person subject to this chapter who intentionally, as a method of warfare, employs a substance or weapon that releases a substance that causes death or serious and lasting damage to health in the ordinary course of events, through its asphyxiating, bacteriological, or toxic properties, shall be punished, if death results to one or more of the victims, by death or such other punishment as a military commission under this chapter may direct, and, if death does not result to any of the victims, by such punishment, other than death, as a military commission under this chapter may direct.

(9) USING PROTECTED PERSONS AS A SHIELD.—Any person subject to this chapter who positions, or otherwise takes advantage of, a protected person with the intent to shield a military objective from attack, or to shield, favor, or impede military operations, shall be punished, if death results to one or more of the victims, by death or such other punishment as a military commission under this chapter may direct, and, if death does not result to any of the victims, by such punishment, other than death, as a military commission under this chapter may direct.

(10) USING PROTECTED PROPERTY AS A SHIELD.—Any person subject to this chapter who positions, or otherwise takes advantage of the location of, protected property with the intent to shield a military objective from attack, or to shield, favor, or impede military operations, shall be punished as a military commission under this chapter may direct.

(11) TORTURE.—

(A) OFFENSE.—Any person subject to this chapter who commits an act specifically intended to inflict severe physical or mental pain or suffering (other than pain or suffering incidental to lawful sanctions) upon another person within his custody or physical control for the purpose of obtaining information or a confession, punishment, intimidation, coercion, or any reason based on discrimination of any kind, shall be punished, if death results to one or more of the victims, by death or such other punishment as a military commission under this chapter may direct, and, if death does not result to any of the victims, by such punishment, other than death, as a military commission under this chapter may direct.

(B) SEVERE MENTAL PAIN OR SUFFERING DEFINED.—In this paragraph, the term “severe mental pain or suffering” has the meaning given that term in section 2340(2) of title 18.

(12) CRUEL OR INHUMAN TREATMENT.—Any person subject to this chapter who subjects another person in their custody or under their physical control, regardless of nationality or physical location, to cruel or inhuman treatment that constitutes a grave breach of common Article 3 of the Geneva Conventions shall be punished, if death results to the victim, by death or such other punishment as a military commission under this chapter may direct, and, if death does not result to the victim, by such punishment, other than death, as a military commission under this chapter may direct.

(13) INTENTIONALLY CAUSING SERIOUS BODILY INJURY.—

(A) OFFENSE.—Any person subject to this chapter who intentionally causes serious bodily injury to one or more persons, including privileged belligerents, in violation of the law of war shall be punished, if death results to one or more of the victims, by death or such other punishment as a military commission under this chapter may direct, and, if death does not result to any of the victims, by such punishment, other than death, as a military commission under this chapter may direct.

(B) SERIOUS BODILY INJURY DEFINED.—In this paragraph, the term “serious bodily injury” means bodily injury which involves—

- (i) a substantial risk of death;
- (ii) extreme physical pain;
- (iii) protracted and obvious disfigurement; or
- (iv) protracted loss or impairment of the function of a bodily member, organ, or mental faculty.

(14) MUTILATING OR MAIMING.—Any person subject to this chapter who intentionally injures one or more protected persons by disfiguring the person or persons by any mutilation of the person or persons, or by permanently disabling any member, limb, or organ of the body of the person or persons, without any

legitimate medical or dental purpose, shall be punished, if death results to one or more of the victims, by death or such other punishment as a military commission under this chapter may direct, and, if death does not result to any of the victims, by such punishment, other than death, as a military commission under this chapter may direct.

(15) MURDER IN VIOLATION OF THE LAW OF WAR.—Any person subject to this chapter who intentionally kills one or more persons, including privileged belligerents, in violation of the law of war shall be punished by death or such other punishment as a military commission under this chapter may direct.

(16) DESTRUCTION OF PROPERTY IN VIOLATION OF THE LAW OF WAR.—Any person subject to this chapter who intentionally destroys property belonging to another person in violation of the law of war shall be punished as a military commission under this chapter may direct.

(17) USING TREACHERY OR PERFIDY.—Any person subject to this chapter who, after inviting the confidence or belief of one or more persons that they were entitled to, or obliged to accord, protection under the law of war, intentionally makes use of that confidence or belief in killing, injuring, or capturing such person or persons shall be punished, if death results to one or more of the victims, by death or such other punishment as a military commission under this chapter may direct, and, if death does not result to any of the victims, by such punishment, other than death, as a military commission under this chapter may direct.

(18) IMPROPERLY USING A FLAG OF TRUCE.—Any person subject to this chapter who uses a flag of truce to feign an intention to negotiate, surrender, or otherwise suspend hostilities when there is no such intention shall be punished as a military commission under this chapter may direct.

(19) IMPROPERLY USING A DISTINCTIVE EMBLEM.—Any person subject to this chapter who intentionally uses a distinctive emblem recognized by the law of war for combatant purposes in a manner prohibited by the law of war shall be punished as a military commission under this chapter may direct.

(20) INTENTIONALLY MISTREATING A DEAD BODY.—Any person subject to this chapter who intentionally mistreats the body of a dead person, without justification by legitimate military necessary, shall be punished as a military commission under this chapter may direct.

(21) RAPE.—Any person subject to this chapter who forcibly or with coercion or threat of force wrongfully invades the body of a person by penetrating, however slightly, the anal or genital opening of the victim with any part of the body of the accused, or with any foreign object, shall be punished as a military commission under this chapter may direct.

(22) SEXUAL ASSAULT OR ABUSE.—Any person subject to this chapter who forcibly or with coercion or threat of force engages in sexual contact with one or

TITLE 10, MILITARY COMMISSIONS

more persons, or causes one or more persons to engage in sexual contact, shall be punished as a military commission under this chapter may direct.

(23) HIJACKING OR HAZARDING A VESSEL OR AIRCRAFT.—Any person subject to this chapter who intentionally seizes, exercises unauthorized control over, or endangers the safe navigation of a vessel or aircraft that is not a legitimate military objective shall be punished, if death results to one or more of the victims, by death or such other punishment as a military commission under this chapter may direct, and, if death does not result to any of the victims, by such punishment, other than death, as a military commission under this chapter may direct.

(24) TERRORISM.—Any person subject to this chapter who intentionally kills or inflicts great bodily harm on one or more protected persons, or intentionally engages in an act that evinces a wanton disregard for human life, in a manner calculated to influence or affect the conduct of government or civilian population by intimidation or coercion, or to retaliate against government conduct, shall be punished, if death results to one or more of the victims, by death or such other punishment as a military commission under this chapter may direct, and, if death does not result to any of the victims, by such punishment, other than death, as a military commission under this chapter may direct.

(25) PROVIDING MATERIAL SUPPORT FOR TERRORISM.—

(A) OFFENSE.—Any person subject to this chapter who provides material support or resources, knowing or intending that they are to be used in preparation for, or in carrying out, an act of terrorism (as set forth in paragraph (24) of this section), or who intentionally provides material support or resources to an international terrorist organization engaged in hostilities against the United States, knowing that such organization has engaged or engages in terrorism (as so set forth), shall be punished as a military commission under this chapter may direct.

(B) MATERIAL SUPPORT OR RESOURCES DEFINED.—In this paragraph, the term “material support or resources” has the meaning given that term in section 2339A(b) of title 18.

(26) WRONGFULLY AIDING THE ENEMY.—Any person subject to this chapter who, in breach of an allegiance or duty to the United States, knowingly and intentionally aids an enemy of the United States, or one of the co-belligerents of the enemy, shall be punished as a military commission under this chapter may direct.

(27) SPYING.—Any person subject to this chapter who, in violation of the law of war and with intent or reason to believe that it is to be used to the injury of the United States or to the advantage of a foreign power, collects or attempts to collect information by clandestine means or while acting under false pretenses, for the purpose of conveying such information to an enemy of the United States,

TITLE 10, MILITARY COMMISSIONS

or one of the co-belligerents of the enemy, shall be punished by death or such other punishment as a military commission under this chapter may direct.

(28) ATTEMPTS.—

(A) IN GENERAL.—Any person subject to this chapter who attempts to commit any offense punishable by this chapter shall be punished as a military commission under this chapter may direct.

(B) SCOPE OF OFFENSE.—An act, done with specific intent to commit an offense under this chapter, amounting to more than mere preparation and tending, even though failing, to effect its commission, is an attempt to commit that offense.

(C) EFFECT OF CONSUMMATION.—Any person subject to this chapter may be convicted of an attempt to commit an offense although it appears on the trial that the offense was consummated.

(29) CONSPIRACY.—Any person subject to this chapter who conspires to commit one or more substantive offenses triable by military commission under this subchapter, and who knowingly does any overt act to effect the object of the conspiracy, shall be punished, if death results to one or more of the victims, by death or such other punishment as a military commission under this chapter may direct, and, if death does not result to any of the victims, by such punishment, other than death, as a military commission under this chapter may direct.

(30) SOLICITATION.—Any person subject to this chapter who solicits or advises another or others to commit one or more substantive offenses triable by military commission under this chapter shall, if the offense solicited or advised is attempted or committed, be punished with the punishment provided for the commission of the offense, but, if the offense solicited or advised is not committed or attempted, shall be punished as a military commission under this chapter may direct.

(31) CONTEMPT.—A military commission under this chapter may punish for contempt any person who uses any menacing word, sign, or gesture in its presence, or who disturbs its proceedings by any riot or disorder.

(32) PERJURY AND OBSTRUCTION OF JUSTICE.—A military commission under this chapter may try offenses and impose such punishment as the military commission may direct for perjury, false testimony, or obstruction of justice related to the military commission.

E-GOVERNMENT ACT OF 2002^[1]

[Public Law 107-347; 116 STAT. 2899; December 17, 2002]

AN ACT To enhance the management and promotion of electronic Government services and processes by establishing a Federal Chief Information Officer within the Office of Management and Budget, and by establishing a broad framework of measures that require using Internet-based information technology to enhance citizen access to Government information and services, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SHORT TITLE; TABLE OF CONTENTS

SECTION I.

(a) SHORT TITLE.—This Act may be cited as the “E-Government Act of 2002”.

(b) TABLE OF CONTENTS.—The table of contents for this Act is as follows:

TITLE I – OFFICE OF MANAGEMENT AND BUDGET ELECTRONIC GOVERNMENT SERVICES

SEC. 101. Short title; table of contents.

TITLE II – FEDERAL MANAGEMENT AND PROMOTION OF ELECTRONIC GOVERNMENT SERVICES

SEC. 208. Privacy provisions.

SEC. 302. Management of information technology.

TITLE II – FEDERAL MANAGEMENT AND PROMOTION OF ELECTRONIC GOVERNMENT SERVICES

PRIVACY PROVISIONS

SEC. 208. [44 U.S.C. 3501 note]

¹ Only select provisions are included, as reflected in the table of contents excerpt.

(a) **PURPOSE.**—The purpose of this section is to ensure sufficient protections for the privacy of personal information as agencies implement citizen-centered electronic Government.

(b) **PRIVACY IMPACT ASSESSMENTS.**—

(1) **RESPONSIBILITIES OF AGENCIES.**—

(A) **IN GENERAL.**—An agency shall take actions described under subparagraph (B) before—

(i) developing or procuring information technology that collects, maintains, or disseminates information that is in an identifiable form; or

(ii) initiating a new collection of information that—
(I) will be collected, maintained, or disseminated using information technology; and
(II) includes any information in an identifiable form permitting the physical or online contacting of a specific individual, if identical questions have been posed to, or identical reporting requirements imposed on, 10 or more persons, other than agencies, instrumentalities, or employees of the Federal Government.

(B) **AGENCY ACTIVITIES.**—To the extent required under subparagraph (A), each agency shall—

(i) conduct a privacy impact assessment;

(ii) ensure the review of the privacy impact assessment by the Chief Information Officer, or equivalent official, as determined by the head of the agency; and

(iii) if practicable, after completion of the review under clause (ii), make the privacy impact assessment publicly available through the website of the agency, publication in the Federal Register, or other means.

(C) **SENSITIVE INFORMATION.**—Subparagraph (B)(iii) may be modified or waived for security reasons, or to protect classified, sensitive, or private information contained in an assessment.

(D) **COPY TO DIRECTOR.**—Agencies shall provide the Director with a copy of the privacy impact assessment for each system for which funding is requested.

(2) **CONTENTS OF A PRIVACY IMPACT ASSESSMENT.**—

(A) **IN GENERAL.**—The Director shall issue guidance to agencies specifying the required contents of a privacy impact assessment.

(B) **GUIDANCE.**—The guidance shall—

- (i) ensure that a privacy impact assessment is commensurate with the size of the information system being assessed, the sensitivity of information that is in an identifiable form in that system, and the risk of harm from unauthorized release of that information; and
- (ii) require that a privacy impact assessment address—
 - (I) what information is to be collected;
 - (II) why the information is being collected;
 - (III) the intended use of the agency of the information;
 - (IV) with whom the information will be shared;
 - (V) what notice or opportunities for consent would be provided to individuals regarding what information is collected and how that information is shared;
 - (VI) how the information will be secured; and
 - (VII) whether a system of records is being created under section 552a of title 5, United States Code, (commonly referred to as the “Privacy Act”).

(3) RESPONSIBILITIES OF THE DIRECTOR.—The Director shall—

- (A) develop policies and guidelines for agencies on the conduct of privacy impact assessments;
- (B) oversee the implementation of the privacy impact assessment process throughout the Government; and
- (C) require agencies to conduct privacy impact assessments of existing information systems or ongoing collections of information that is in an identifiable form as the Director determines appropriate.

(c) PRIVACY PROTECTIONS ON AGENCY WEBSITES.—

(1) PRIVACY POLICIES ON WEBSITES.—

(A) GUIDELINES FOR NOTICES.—The Director shall develop guidance for privacy notices on agency websites used by the public.

(B) CONTENTS.—The guidance shall require that a privacy notice address, consistent with section 552a of title 5, United States Code—

- (i) what information is to be collected;
- (ii) why the information is being collected;
- (iii) the intended use of the agency of the information;
- (iv) with whom the information will be shared;

(v) what notice or opportunities for consent would be provided to individuals regarding what information is collected and how that information is shared;

(vi) how the information will be secured; and

(vii) the rights of the individual under section 552a of title 5, United States Code (commonly referred to as the 'Privacy Act'), and other laws relevant to the protection of the privacy of an individual.

(2) **PRIVACY POLICIES IN MACHINE-READABLE FORMATS.**—The Director shall issue guidance requiring agencies to translate privacy policies into a standardized machine-readable format.

(d) **DEFINITION.**—In this section, the term “identifiable form” means any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means.

MANAGEMENT OF INFORMATION TECHNOLOGY

SEC. 302. [Amending 40 U.S.C. § 11331 to read as follows:]

SEC. 11331. RESPONSIBILITIES FOR FEDERAL INFORMATION SYSTEMS STANDARDS.

(a) **DEFINITION.**—In this section, the term “information security” has the meaning given that term in section 3532(b)(1) of title 44.

(b) **REQUIREMENT TO PRESCRIBE STANDARDS.**

(1) **IN GENERAL.**—

(A) **REQUIREMENT.**—Except as provided under paragraph (2), the Director of the Office of Management and Budget shall, on the basis of proposed standards developed by the National Institute of Standards and Technology pursuant to paragraphs (2) and (3) of section 20(a) of the National Institute of Standards and Technology Act (15 U.S.C. 278g-3(a)) and in consultation with the Secretary of Homeland Security, promulgate information security standards pertaining to Federal information systems.

(B) **REQUIRED STANDARDS.**—Standards promulgated under subparagraph (A) shall include—

(i) standards that provide minimum information security requirements as determined under section 20(b) of the National Institute of Standards and Technology Act (15 U.S.C. 278g-3(b)); and

(ii) such standards that are otherwise necessary to improve the efficiency of operation or security of Federal information systems.

(C) REQUIRED STANDARDS BINDING.—Information security standards described under subparagraph (B) shall be compulsory and binding.

(c) APPLICATION OF MORE STRINGENT STANDARDS.—The head of an agency may employ standards for the cost-effective information security for all operations and assets within or under the supervision of that agency that are more stringent than the standards promulgated by the Director under this section, if such standards—

(1) contain, at a minimum, the provisions of those applicable standards made compulsory and binding by the Director; and

(2) are otherwise consistent with policies and guidelines issued under section 3533 of title 44.

(d) REQUIREMENTS REGARDING DECISIONS BY DIRECTOR.—

(1) DEADLINE. —The decision regarding the promulgation of any standard by the Director under subsection (b) shall occur not later than 6 months after the submission of the proposed standard to the Director by the National Institute of Standards and Technology, as provided under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g-3).

(2) NOTICE AND COMMENT. —A decision by the Director to significantly modify, or not promulgate a proposed standard submitted to the Director by the National Institute of Standards and Technology, as provided under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g-3), shall be made after the public is given an opportunity to comment on the Director's proposed decision.

FEDERAL AGENCY DATA MINING REPORTING ACT OF 2007

[Section 804 of the Implementing Recommendations of the
9/11 Commission Act of 2007]
[Public Law 110-53; 121 STAT. 362; August 3, 2007]

SEC. 804. [42 U.S.C. § 2000ee-3]

(a) **SHORT TITLE.**—This section may be cited as the “Federal Agency Data Mining Reporting Act of 2007”.

(b) **DEFINITIONS.**—In this section:

(1) **DATA MINING.**—The term “data mining” means a program involving pattern-based queries, searches, or other analyses of 1 or more electronic databases, where—

(A) a department or agency of the Federal Government, or a non-Federal entity acting on behalf of the Federal Government, is conducting the queries, searches, or other analyses to discover or locate a predictive pattern or anomaly indicative of terrorist or criminal activity on the part of any individual or individuals;

(B) the queries, searches, or other analyses are not subject-based and do not use personal identifiers of a specific individual, or inputs associated with a specific individual or group of individuals, to retrieve information from the database or databases; and

(C) the purpose of the queries, searches, or other analyses is not solely—

(i) the detection of fraud, waste, or abuse in a Government agency or program; or

(ii) the security of a Government computer system.

(2) **DATABASE.**—The term “database” does not include telephone directories, news reporting, information publicly available to any member of the public without payment of a fee, or databases of judicial and administrative opinions or other legal research sources.

(c) **REPORTS ON DATA MINING ACTIVITIES BY FEDERAL AGENCIES.**—

(1) **REQUIREMENT FOR REPORT.**—The head of each department or agency of the Federal Government that is engaged in any activity to use or develop data mining shall submit a report to Congress on all such activities of the department or agency under the jurisdiction of that official. The report shall be produced in coordination with the privacy officer of that department or agency, if applicable, and shall be made

available to the public, except for an annex described in subparagraph (C).

(2) **CONTENT OF REPORT.**—Each report submitted under subparagraph (A) shall include, for each activity to use or develop data mining, the following information:

(A) A thorough description of the data mining activity, its goals, and, where appropriate, the target dates for the deployment of the data mining activity.

(B) A thorough description of the data mining technology that is being used or will be used, including the basis for determining whether a particular pattern or anomaly is indicative of terrorist or criminal activity.

(C) A thorough description of the data sources that are being or will be used.

(D) An assessment of the efficacy or likely efficacy of the data mining activity in providing accurate information consistent with and valuable to the stated goals and plans for the use or development of the data mining activity.

(E) An assessment of the impact or likely impact of the implementation of the data mining activity on the privacy and civil liberties of individuals, including a thorough description of the actions that are being taken or will be taken with regard to the property, privacy, or other rights or privileges of any individual or individuals as a result of the implementation of the data mining activity.

(F) A list and analysis of the laws and regulations that govern the information being or to be collected, reviewed, gathered, analyzed, or used in conjunction with the data mining activity, to the extent applicable in the context of the data mining activity.

(G) A thorough discussion of the policies, procedures, and guidelines that are in place or that are to be developed and applied in the use of such data mining activity in order to—

(i) protect the privacy and due process rights of individuals, such as redress procedures; and

(ii) ensure that only accurate and complete information is collected, reviewed, gathered, analyzed, or used, and guard against any harmful consequences of potential inaccuracies.

(3) **ANNEX.**—

(A) **IN GENERAL.**—A report under subparagraph (A) shall include in an annex any necessary—

- (i) classified information;
 - (ii) law enforcement sensitive information;
 - (iii) proprietary business information; or
 - (iv) trade secrets (as that term is defined in section 1839 of title 18, United States Code).
- (B) AVAILABILITY.—Any annex described in clause (i)—
- (i) shall be available, as appropriate, and consistent with the National Security Act of 1947 (50 U.S.C. 401 et seq.), to the Committee on Homeland Security and Governmental Affairs, the Committee on the Judiciary, the Select Committee on Intelligence, the Committee on Appropriations, and the Committee on Banking, Housing, and Urban Affairs of the Senate and the Committee on Homeland Security, the Committee on the Judiciary, the Permanent Select Committee on Intelligence, the Committee on Appropriations, and the Committee on Financial Services of the House of Representatives; and
 - (ii) shall not be made available to the public.
- (4) TIME FOR REPORT.—Each report required under subparagraph (A) shall be—
- (A) submitted not later than 180 days after the date of enactment of this Act; and
 - (B) updated not less frequently than annually thereafter, to include any activity to use or develop data mining engaged in after the date of the prior report submitted under subparagraph (A).

**FEDERAL INFORMATION SECURITY
MODERNIZATION ACT [FISMA] OF 2014^[1]**

[Public Law 113-283; 128 STAT. 3073; December 18, 2014]

AN ACT To amend chapter 35 of title 44, United States Code, to provide for reform to Federal information security.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

TABLE OF CONTENTS²

SEC. 1. Short title.

SEC. 2. Amending the following sections of title 44, United States Code:

SEC. 3551. Purpose.

SEC. 3552. Definitions.

SEC. 3553. Authority and functions of the Director and the Secretary.

SEC. 3554. Federal agency responsibilities.

SEC. 3555. Annual independent evaluation.

SEC. 3556. Federal Information Security Incident Center.

SEC. 3557. National Security Systems.

SEC. 3558. Effect on existing law.

SHORT TITLE

SECTION. 1.

This Act may be cited as the “Federal Information Security Modernization Act of 2014.

SEC. 2. [Amending 44 U.S.C. §§ 3551-3558 to read as follows:]

PURPOSES

SEC. 3551.

The purposes of this subchapter are to—

¹ Only select provisions are included, as reflected in the table of contents.

² Table of Contents does not appear in the Act itself.

- (1) provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets;
- (2) recognize the highly networked nature of the current Federal computing environment and provide effective governmentwide management and oversight of the related information security risks, including coordination of information security efforts throughout the civilian, national security, and law enforcement communities;
- (3) provide for development and maintenance of minimum controls required to protect Federal information and information systems;
- (4) provide a mechanism for improved oversight of Federal agency information security programs, including through automated security tools to continuously diagnose and improve security;
- (5) acknowledge that commercially developed information security products offer advanced, dynamic, robust, and effective information security solutions, reflecting market solutions for the protection of critical information infrastructures important to the national defense and economic security of the nation that are designed, built, and operated by the private sector; and
- (6) recognize that the selection of specific technical hardware and software information security solutions should be left to individual agencies from among commercially developed products.

DEFINITIONS

SEC. 3552.

(a) **IN GENERAL.**—Except as provided under subsection (b), the definitions under section 3502 shall apply to this subchapter.

(b) **ADDITIONAL DEFINITIONS.**—As used in this subchapter:

(1) The term “binding operational directive” means a compulsory direction to an agency that—

(A) is for purposes of safeguarding Federal information and information systems from a known or reasonably suspected information security threat, vulnerability, or risk;

(B) shall be in accordance with policies, principles, standards, and guidelines issued by the Director; and

(C) may be revised or repealed by the Director if the direction issued on behalf of the Director is not in accordance with policies and principles developed by the Director.

- (2) The term “incident” means an occurrence that—
- (A) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or
 - (B) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.
- (3) The term “information security” means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide—
- (A) integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity;
 - (B) confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and
 - (C) availability, which means ensuring timely and reliable access to and use of information.
- (4) The term “information technology” has the meaning given that term in section 11101 of title 40.
- (5) The term “intelligence community” has the meaning given that term in section 3(4) of the National Security Act of 1947 (50 U.S.C. 3003(4)).
- (6)(A) The term “national security system” means any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency—
- (i) the function, operation, or use of which—
 - (I) involves intelligence activities;
 - (II) involves cryptologic activities related to national security;
 - (III) involves command and control of military forces;
 - (IV) involves equipment that is an integral part of a weapon or weapons system; or
 - (V) subject to subparagraph (B), is critical to the direct fulfillment of military or intelligence missions; or
 - (ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.

(B) Subparagraph (A)(i)(V) does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications).

(7) The term “Secretary” means the Secretary of Homeland Security.

AUTHORITY AND FUNCTIONS OF THE DIRECTOR AND THE SECRETARY

SEC. 3553.

(a) **DIRECTOR.**—The Director shall oversee agency information security policies and practices, including—

(1) developing and overseeing the implementation of policies, principles, standards, and guidelines on information security, including through ensuring timely agency adoption of and compliance with standards promulgated under section 11331 of title 40;

(2) requiring agencies, consistent with the standards promulgated under such section 11331 and the requirements of this subchapter, to identify and provide information security protections commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of—

(A) information collected or maintained by or on behalf of an agency; or

(B) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency;

(3) ensuring that the Secretary carries out the authorities and functions under subsection (b);

(4) coordinating the development of standards and guidelines under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3) with agencies and offices operating or exercising control of national security systems (including the National Security Agency) to assure, to the maximum extent feasible, that such standards and guidelines are complementary with standards and guidelines developed for national security systems;

(5) overseeing agency compliance with the requirements of this subchapter and section 1326 of title 41, including through any authorized action under section 11303 of title 40, to enforce accountability for compliance with such requirements; and

(6) coordinating information security policies and procedures with related information resources management policies and procedures.

(b) SECRETARY.—The Secretary, in consultation with the Director, shall administer the implementation of agency information security policies and practices for information systems, except for national security systems and information systems described in paragraph (2) or (3) of subsection (e), including—

- (1) assisting the Director in carrying out the authorities and functions under paragraphs (1), (2), (3), (5), and (6) of subsection (a);
- (2) developing and overseeing the implementation of binding operational directives to agencies to implement the policies, principles, standards, and guidelines developed by the Director under subsection (a)(1) and the requirements of this subchapter, which may be revised or repealed by the Director if the operational directives issued on behalf of the Director are not in accordance with policies, principles, standards, and guidelines developed by the Director, including—
 - (A) requirements for reporting security incidents to the Federal information security incident center established under section 3556;
 - (B) requirements for the contents of the annual reports required to be submitted under section 3554(c)(1);
 - (C) requirements for the mitigation of exigent risks to information systems; and
 - (D) other operational requirements as the Director or Secretary, in consultation with the Director, may determine necessary;
- (3) monitoring agency implementation of information security policies and practices;
- (4) convening meetings with senior agency officials to help ensure effective implementation of information security policies and practices;
- (5) coordinating Government-wide efforts on information security policies and practices, including consultation with the Chief Information Officers Council established under section 3603 and the Director of the National Institute of Standards and Technology;
- (6) providing operational and technical assistance to agencies in implementing policies, principles, standards, and guidelines on information security, including implementation of standards promulgated under section 11331 of title 40, including by—
 - (A) operating the Federal information security incident center established under section 3556;
 - (B) upon request by an agency, deploying, operating, and maintaining technology to assist the agency to continuously diagnose and mitigate against cyber threats and vulnerabilities, with or without reimbursement;

(C) compiling and analyzing data on agency information security; and

(D) developing and conducting targeted operational evaluations, including threat and vulnerability assessments, on the information systems;

(7) hunting for and identifying, with or without advance notice to or authorization from agencies, threats and vulnerabilities within Federal information systems;

(8) upon request by an agency, and at the Secretary's discretion, with or without reimbursement—

(A) providing services, functions, and capabilities, including operation of the agency's information security program, to assist the agency with meeting the requirements set forth in section 3554(b); and

(B) deploying, operating, and maintaining secure technology platforms and tools, including networks and common business applications, for use by the agency to perform agency functions, including collecting, maintaining, storing, processing, disseminating, and analyzing information; and

(9) other actions as the Director or the Secretary, in consultation with the Director, may determine necessary to carry out this subsection.

(c) REPORT.—Not later than March 1 of each year, the Director, in consultation with the Secretary, shall submit to Congress a report on the effectiveness of information security policies and practices during the preceding year, including—

(1) a summary of the incidents described in the annual reports required to be submitted under section 3554(c)(1), including a summary of the information required under section 3554(c)(1)(A)(iii);

(2) a description of the threshold for reporting major information security incidents;

(3) a summary of the results of evaluations required to be performed under section 3555;

(4) an assessment of agency compliance with standards promulgated under section 11331 of title 40; and

(5) an assessment of agency compliance with data breach notification policies and procedures issued by the Director.

(d) NATIONAL SECURITY SYSTEMS.—Except for the authorities and functions described in subsection (a)(5) and subsection (c), the authorities and functions of the Director and the Secretary under this section shall not apply to national security systems.

(e) DEPARTMENT OF DEFENSE AND INTELLIGENCE COMMUNITY SYSTEMS.—

(1) The authorities of the Director described in paragraphs (1) and (2) of subsection (a) shall be delegated to the Secretary of Defense in the case of systems described in paragraph (2) and to the Director of National Intelligence in the case of systems described in paragraph (3).

(2) The systems described in this paragraph are systems that are operated by the Department of Defense, a contractor of the Department of Defense, or another entity on behalf of the Department of Defense that processes any information the unauthorized access, use, disclosure, disruption, modification, or destruction of which would have a debilitating impact on the mission of the Department of Defense.

(3) The systems described in this paragraph are systems that are operated by an element of the intelligence community, a contractor of an element of the intelligence community, or another entity on behalf of an element of the intelligence community that processes any information the unauthorized access, use, disclosure, disruption, modification, or destruction of which would have a debilitating impact on the mission of an element of the intelligence community.

(f) CONSIDERATION.—

(1) IN GENERAL.—In carrying out the responsibilities under subsection (b), the Secretary shall consider any applicable standards or guidelines developed by the National Institute of Standards and Technology and issued by the Secretary of Commerce under section 11331 of title 40.

(2) DIRECTIVES.—The Secretary shall—

(A) consult with the Director of the National Institute of Standards and Technology regarding any binding operational directive that implements standards and guidelines developed by the National Institute of Standards and Technology; and

(B) ensure that binding operational directives issued under subsection (b)(2) do not conflict with the standards and guidelines issued under section 11331 of title 40.

(3) RULE OF CONSTRUCTION. —Nothing in this subchapter shall be construed as authorizing the Secretary to direct the Secretary of Commerce in the development and promulgation of standards and guidelines under section 11331 of title 40.

(g) EXERCISE OF AUTHORITY.—To ensure fiscal and policy consistency, the Secretary shall exercise the authority under this section subject to direction by the President, in coordination with the Director.

(h) DIRECTION TO AGENCIES.—

(1) AUTHORITY.—

(A) IN GENERAL.—Subject to subparagraph (B), in response to a known or reasonably suspected information security threat, vulnerability, or incident that represents a substantial threat to the information security of an agency, the Secretary may issue an emergency directive to the head of an agency to take any lawful action with respect to the operation of the information system, including such systems used or operated by another entity on behalf of an agency, that collects, processes, stores, transmits, disseminates, or otherwise maintains agency information, for the purpose of protecting the information system from, or mitigating, an information security threat.

(B) EXCEPTION.—The authorities of the Secretary under this subsection shall not apply to a system described subsection (d) or to a system described in paragraph (2) or (3) of subsection (e).

(2) PROCEDURES FOR USE OF AUTHORITY.—The Secretary shall—

(A) in coordination with the Director, and in consultation with Federal contractors as appropriate, establish procedures governing the circumstances under which a directive may be issued under this subsection, which shall include—

(i) thresholds and other criteria;

(ii) privacy and civil liberties protections; and

(iii) providing notice to potentially affected third parties;

(B) specify the reasons for the required action and the duration of the directive;

(C) minimize the impact of a directive under this subsection by—

(i) adopting the least intrusive means possible under the circumstances to secure the agency information systems; and

(ii) limiting directives to the shortest period practicable;

(D) notify the Director and the head of any affected agency immediately upon the issuance of a directive under this subsection;

(E) consult with the Director of the National Institute of Standards and Technology regarding any directive under this subsection that implements standards and guidelines developed by the National Institute of Standards and Technology;

(F) ensure that directives issued under this subsection do not conflict with the standards and guidelines issued under section 11331 of title 40;

(G) consider any applicable standards or guidelines developed by the National Institute of Standards and Technology issued by the Secretary of Commerce under section 11331 of title 40; and

(H) not later than February 1 of each year, submit to the appropriate congressional committees a report regarding the specific actions the Secretary has taken pursuant to paragraph (1)(A).

(3) IMMINENT THREATS.—

(A) IN GENERAL.—Notwithstanding section 3554, the Secretary may authorize the use under this subsection of the intrusion detection and prevention capabilities established under section 230(b)(1) of the Homeland Security Act of 2002 for the purpose of ensuring the security of agency information systems, if—

(i) the Secretary determines there is an imminent threat to agency information systems;

(ii) the Secretary determines a directive under subsection (b)(2)(C) or paragraph (1)(A) is not reasonably likely to result in a timely response to the threat;

(iii) the Secretary determines the risk posed by the imminent threat outweighs any adverse consequences reasonably expected to result from the use of the intrusion detection and prevention capabilities under the control of the Secretary;

(iv) the Secretary provides prior notice to the Director, and the head and chief information officer (or equivalent official) of each agency to which specific actions will be taken pursuant to this paragraph, and notifies the appropriate congressional committees and authorizing committees of each such agency within 7 days of taking an action under this paragraph of—

(I) any action taken under this paragraph; and

(II) the reasons for and duration and nature of the action;

(v) the action of the Secretary is consistent with applicable law; and

(vi) the Secretary authorizes the use of the intrusion detection and prevention capabilities in accordance with

the advance procedures established under subparagraph (C).

(B) LIMITATION ON DELEGATION.—The authority under this paragraph may not be delegated by the Secretary.

(C) ADVANCE PROCEDURES.—The Secretary shall, in coordination with the Director, and in consultation with the heads of Federal agencies, establish procedures governing the circumstances under which the Secretary may authorize the use of the intrusion detection and prevention capabilities under subparagraph (A). The Secretary shall submit the procedures to Congress.

(4) LIMITATION.—The Secretary may direct or authorize lawful action or the use of the intrusion detection and prevention capabilities under this subsection only to—

(A) protect agency information from unauthorized access, use, disclosure, disruption, modification, or destruction; or

(B) require the remediation of or protect against identified information security risks with respect to—

(i) information collected or maintained by or on behalf of an agency; or

(ii) that portion of an information system used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency.

(i) ANNUAL REPORT TO CONGRESS.—Not later than February 1 of each year, the Director and the Secretary shall submit to the appropriate congressional committees a report regarding the specific actions the Director and the Secretary have taken pursuant to subsection (a)(5), including any actions taken pursuant to section 11303(b)(5) of title 40.

(j) RULE OF CONSTRUCTION.—Nothing in this section shall be construed to require the Secretary to provide notice to any private entity before the Secretary issues a binding operational directive under subsection (b)(2).

(k) APPROPRIATE CONGRESSIONAL COMMITTEES DEFINED.—In this section, the term “appropriate congressional committees” means—

(1) the Committee on Appropriations and the Committee on Homeland Security and Governmental Affairs of the Senate; and

(2) the Committee on Appropriations, the Committee on Homeland Security, the Committee on Oversight and Government Reform, and the Committee on Science, Space, and Technology of the House of Representatives.

(I) INFORMATION SHARING. —

(1) IN GENERAL.—Notwithstanding any other provision of law, including any provision of law that would otherwise restrict or prevent the head of an agency from disclosing information to the Secretary, the Secretary in carrying out this section and title XXII of the Homeland Security Act of 2002 (6 U.S.C. 651 et seq.) may access, use, retain, and disclose, and the head of an agency may disclose to the Secretary, information, for the purpose of protecting information and information systems from cybersecurity risks.

(2) EXCEPTION.—Paragraph (1) shall not apply to national security systems or to information systems described in paragraph (2) or (3) of subsection (e).

FEDERAL AGENCY RESPONSIBILITIES

SEC. 3554.

(a) IN GENERAL.—The head of each agency shall—

(1) be responsible for—

(A) providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of—

(i) information collected or maintained by or on behalf of the agency; and

(ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency;

(B) complying with the requirements of this subchapter, subchapter III of chapter 13 of title 41, and related policies, procedures, standards, and guidelines, including—

(i) information security standards promulgated under section 11331 of title 40;

(ii) operational directives developed by the Secretary under section 3553(b);

(iii) policies and procedures issued by the Director;

(iv) information security standards and guidelines for national security systems issued in accordance with law and as directed by the President; and

(v) emergency directives issued by the Secretary under section 3553(h);

- (vi) responsibilities relating to assessing and avoiding, mitigating, transferring, or accepting supply chain risks under section 1326 of title 41, and complying with exclusion and removal orders issued under section 1323 of such title; and
 - (C) ensuring that information security management processes are integrated with agency strategic, operational, and budgetary planning processes;
- (2) ensure that senior agency officials provide information security for the information and information systems that support the operations and assets under their control, including through—
 - (A) assessing the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of such information or information systems;
 - (B) determining the levels of information security appropriate to protect such information and information systems in accordance with standards promulgated under section 11331 of title 40, for information security classifications and related requirements;
 - (C) implementing policies and procedures to cost-effectively reduce risks to an acceptable level; and
 - (D) periodically testing and evaluating information security controls and techniques to ensure that they are effectively implemented;
- (3) delegate to the agency Chief Information Officer established under section 3506 (or comparable official in an agency not covered by such section) the authority to ensure compliance with the requirements imposed on the agency under this subchapter, including—
 - (A) designating a senior agency information security officer who shall—
 - (i) carry out the Chief Information Officer’s responsibilities under this section;
 - (ii) possess professional qualifications, including training and experience, required to administer the functions described under this section;
 - (iii) have information security duties as that official’s primary duty; and
 - (iv) head an office with the mission and resources to assist in ensuring agency compliance with this section;
 - (B) developing and maintaining an agencywide information security program as required by subsection (b);

(C) developing and maintaining information security policies, procedures, and control techniques to address all applicable requirements, including those issued under section 3553 of this title and section 11331 of title 40;

(D) training and overseeing personnel with significant responsibilities for information security with respect to such responsibilities; and

(E) assisting senior agency officials concerning their responsibilities under paragraph (2);

(4) ensure that the agency has trained personnel sufficient to assist the agency in complying with the requirements of this subchapter and related policies, procedures, standards, and guidelines;

(5) ensure that the agency Chief Information Officer, in coordination with other senior agency officials, reports annually to the agency head on the effectiveness of the agency information security program, including progress of remedial actions;

(6) ensure that senior agency officials, including chief information officers of component agencies or equivalent officials, carry out responsibilities under this subchapter as directed by the official delegated authority under paragraph (3); and

(7) ensure that all personnel are held accountable for complying with the agency-wide information security program implemented under subsection (b).

(b) AGENCY PROGRAM.—Each agency shall develop, document, and implement an agency-wide information security program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source, that includes—

(1) periodic assessments of the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency, which may include using automated tools consistent with standards and guidelines promulgated under section 11331 of title 40;

(2) policies and procedures that—

(A) are based on the risk assessments required by paragraph (1);

(B) cost-effectively reduce information security risks to an acceptable level;

(C) ensure that information security is addressed throughout the life cycle of each agency information system; and

- (D) ensure compliance with—
 - (i) the requirements of this subchapter;
 - (ii) policies and procedures as may be prescribed by the Director, and information security standards promulgated under section 11331 of title 40;
 - (iii) minimally acceptable system configuration requirements, as determined by the agency; and
 - (iv) any other applicable requirements, including standards and guidelines for national security systems issued in accordance with law and as directed by the President;
- (3) subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate;
- (4) security awareness training to inform personnel, including contractors and other users of information systems that support the operations and assets of the agency, of—
 - (A) information security risks associated with their activities; and
 - (B) their responsibilities in complying with agency policies and procedures designed to reduce these risks;
- (5) periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices, to be performed with a frequency depending on risk, but no less than annually, of which such testing—
 - (A) shall include testing of management, operational, and technical controls of every information system identified in the inventory required under section 3505(c);
 - (B) may include testing relied on in an evaluation under section 3555; and
 - (C) shall include using automated tools, consistent with standards and guidelines promulgated under section 11331 of title 40;
- (6) a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices of the agency;
- (7) procedures for detecting, reporting, and responding to security incidents, which—
 - (A) shall be consistent with the standards and guidelines described in section 3556(b);
 - (B) may include using automated tools; and

(C) shall include—

(i) mitigating risks associated with such incidents before substantial damage is done;

(ii) notifying and consulting with the Federal information security incident center established in section 3556; and

(iii) notifying and consulting with, as appropriate—

(I) law enforcement agencies and relevant Offices of Inspector General and Offices of General Counsel;

(II) an office designated by the President for any incident involving a national security system;

(III) for a major incident, the committees of Congress described in subsection (c)(1)—

(aa) not later than 7 days after the date on which there is a reasonable basis to conclude that the major incident has occurred; and

(bb) after the initial notification under item (aa), within a reasonable period of time after additional information relating to the incident is discovered, including the summary required under subsection (c)(1)(A)(i); and

(IV) any other agency or office, in accordance with law or as directed by the President; and

(8) plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency.

(c) AGENCY REPORTING.—

(1) ANNUAL REPORT.—

(A) IN GENERAL.—Each agency shall submit to the Director, the Secretary, the Committee on Government Reform, the Committee on Homeland Security, and the Committee on Science of the House of Representatives, the Committee on Homeland Security and Governmental Affairs and the Committee on Commerce, Science, and Transportation of the Senate, the appropriate authorization and appropriations committees of Congress, and the Comptroller General a report on the adequacy and effectiveness of information security policies, procedures, and practices, including—

(i) a description of each major information security incident or related sets of incidents, including summaries of—

- (I) the threats and threat actors, vulnerabilities, and impacts relating to the incident;
- (II) the risk assessments conducted under section 3554(a)(2)(A) of the affected information systems before the date on which the incident occurred;
- (III) the status of compliance of the affected information systems with applicable security requirements at the time of the incident; and
- (IV) the detection, response, and remediation actions;

(ii) the total number of information security incidents, including a description of incidents resulting in significant compromise of information security, system impact levels, types of incident, and locations of affected systems;

(iii) a description of each major information security incident that involved a breach of personally identifiable information, as defined by the Director, including—

- (I) the number of individuals whose information was affected by the major information security incident; and
- (II) a description of the information that was breached or exposed; and

(iv) any other information as the Director or the Secretary, in consultation with the Director, may require.

(B) UNCLASSIFIED REPORT.—

(i) In general.—Each report submitted under subparagraph (A) shall be in unclassified form, but may include a classified annex.

(ii) Access to information.—The head of an agency shall ensure that, to the greatest extent practicable, information is included in the unclassified version of the reports submitted by the agency under subparagraph (A).

(2) OTHER PLANS AND REPORTS.—Each agency shall address the adequacy and effectiveness of information security policies, procedures, and practices in management plans and reports.

(d) **PERFORMANCE PLAN.**—(1) In addition to the requirements of subsection (c), each agency, in consultation with the Director, shall include as part of the performance plan required under section 1115 of title 31 a description of—

(A) the time periods; and

(B) the resources, including budget, staffing, and training, that are necessary to implement the program required under subsection (b).

(2) The description under paragraph (1) shall be based on the risk assessments required under subsection (b)(1).

(e) **PUBLIC NOTICE AND COMMENT.**—Each agency shall provide the public with timely notice and opportunities for comment on proposed information security policies and procedures to the extent that such policies and procedures affect communication with the public.

ANNUAL INDEPENDENT EVALUATION

SEC. 3555.

(a) **IN GENERAL.**—

(1) Each year each agency shall have performed an independent evaluation of the information security program and practices of that agency to determine the effectiveness of such program and practices.

(2) Each evaluation under this section shall include—

(A) testing of the effectiveness of information security policies, procedures, and practices of a representative subset of the agency's information systems;

(B) an assessment of the effectiveness of the information security policies, procedures, and practices of the agency; and

(C) separate presentations, as appropriate, regarding information security relating to national security systems.

(b) **INDEPENDENT AUDITOR.**—Subject to subsection (c)—

(1) for each agency with an Inspector General appointed under chapter 4 of title 5, the annual evaluation required by this section shall be performed by the Inspector General or by an independent external auditor, as determined by the Inspector General of the agency; and

(2) for each agency to which paragraph (1) does not apply, the head of the agency shall engage an independent external auditor to perform the evaluation.

(c) **NATIONAL SECURITY SYSTEMS.**—For each agency operating or exercising control of a national security system, that portion of the evaluation required by this section directly relating to a national security system shall be performed—

(1) only by an entity designated by the agency head; and

(2) in such a manner as to ensure appropriate protection for information associated with any information security vulnerability in such system commensurate with the risk and in accordance with all applicable laws.

(d) EXISTING EVALUATIONS.—The evaluation required by this section may be based in whole or in part on an audit, evaluation, or report relating to programs or practices of the applicable agency.

(e) AGENCY REPORTING.—

(1) Each year, not later than such date established by the Director, the head of each agency shall submit to the Director the results of the evaluation required under this section.

(2) To the extent an evaluation required under this section directly relates to a national security system, the evaluation results submitted to the Director shall contain only a summary and assessment of that portion of the evaluation directly relating to a national security system.

(f) PROTECTION OF INFORMATION.—Agencies and evaluators shall take appropriate steps to ensure the protection of information which, if disclosed, may adversely affect information security. Such protections shall be commensurate with the risk and comply with all applicable laws and regulations.

(g) OMB REPORTS TO CONGRESS.—

(1) The Director shall summarize the results of the evaluations conducted under this section in the report to Congress required under section 3553(c).

(2) The Director's report to Congress under this subsection shall summarize information regarding information security relating to national security systems in such a manner as to ensure appropriate protection for information associated with any information security vulnerability in such system commensurate with the risk and in accordance with all applicable laws.

(3) Evaluations and any other descriptions of information systems under the authority and control of the Director of National Intelligence or of National Foreign Intelligence Programs systems under the authority and control of the Secretary of Defense shall be made available to Congress only through the appropriate oversight committees of Congress, in accordance with applicable laws.

(h) COMPTROLLER GENERAL.—The Comptroller General shall periodically evaluate and report to Congress on—

(1) the adequacy and effectiveness of agency information security policies and practices; and

(2) implementation of the requirements of this subchapter.

(i) ASSESSMENT TECHNICAL ASSISTANCE.—The Comptroller General may provide technical assistance to an Inspector General or the head of an agency, as

applicable, to assist the Inspector General or head of an agency in carrying out the duties under this section, including by testing information security controls and procedures.

(j) **GUIDANCE.**—The Director, in consultation with the Secretary, the Chief Information Officers Council established under section 3603, the Council of the Inspectors General on Integrity and Efficiency, and other interested parties as appropriate, shall ensure the development of guidance for evaluating the effectiveness of an information security program and practices.

FEDERAL INFORMATION SECURITY INCIDENT CENTER

SEC. 3556.

(a) **IN GENERAL.**—The Secretary shall ensure the operation of a central Federal information security incident center to—

- (1) provide timely technical assistance to operators of agency information systems regarding security incidents, including guidance on detecting and handling information security incidents;
- (2) compile and analyze information about incidents that threaten information security;
- (3) inform operators of agency information systems about current and potential information security threats, and vulnerabilities;
- (4) provide, as appropriate, intelligence and other information about cyber threats, vulnerabilities, and incidents to agencies to assist in risk assessments conducted under section 3554(b); and
- (5) consult with the National Institute of Standards and Technology, agencies or offices operating or exercising control of national security systems (including the National Security Agency), and such other agencies or offices in accordance with law and as directed by the President regarding information security incidents and related matters.

(b) **NATIONAL SECURITY SYSTEMS.**—Each agency operating or exercising control of a national security system shall share information about information security incidents, threats, and vulnerabilities with the Federal information security incident center to the extent consistent with standards and guidelines for national security systems, issued in accordance with law and as directed by the President.

NATIONAL SECURITY SYSTEMS

SEC. 3557.

The head of each agency operating or exercising control of a national security system shall be responsible for ensuring that the agency—

- (1) provides information security protections commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information contained in such system;
- (2) implements information security policies and practices as required by standards and guidelines for national security systems, issued in accordance with law and as directed by the President; and
- (3) complies with the requirements of this subchapter.

EFFECT ON EXISTING LAW

SEC. 3558.

Nothing in this subchapter, section 11331 of title 40, or section 20 of the National Standards and Technology Act (15 U.S.C. 278g–3) may be construed as affecting the authority of the President, the Office of Management and Budget or the Director thereof, the National Institute of Standards and Technology, or the head of any agency, with respect to the authorized use or disclosure of information, including with regard to the protection of personal privacy under section 552a of title 5, the disclosure of information under section 552 of title 5, the management and disposition of records under chapters 29, 31, or 33 of title 44, the management of information resources under subchapter I of chapter 35 of this title, or the disclosure of information to the Congress or the Comptroller General of the United States.

TITLE 40, CHAPTER 113, UNITED STATES CODE,
RESPONSIBILITIES FOR FEDERAL INFORMATION
SYSTEMS STANDARDS

SEC. 11331.

(a) DEFINITION.—In this section, the term “information security” has the meaning given that term in section 3532(b)(1) of title 44.

(b) REQUIREMENT TO PRESCRIBE STANDARDS.—

(1) IN GENERAL.—

(A) REQUIREMENT.—Except as provided under paragraph (2), the Director of the Office of Management and Budget shall, on the basis of proposed standards developed by the National Institute of Standards and Technology pursuant to paragraphs (2) and (3) of section 20(a) of the National Institute of Standards and Technology Act (15 U.S.C. 278g-3(a)) and in consultation with the Secretary of Homeland Security, promulgate information security standards pertaining to Federal information systems.

(B) REQUIRED STANDARDS.—Standards promulgated under subparagraph (A) shall include—

(i) standards that provide minimum information security requirements as determined under section 20(b) of the National Institute of Standards and Technology Act (15 U.S.C. 278g-3(b)); and

(ii) such standards that are otherwise necessary to improve the efficiency of operation or security of Federal information systems.

(C) REQUIRED STANDARDS BINDING.—Information security standards described under subparagraph (B) shall be compulsory and binding.

(2) STANDARDS AND GUIDELINES FOR NATIONAL SECURITY SYSTEMS.—Standards and guidelines for national security systems, as defined under section 3532(3) of title 44, shall be developed, promulgated, enforced, and overseen as otherwise authorized by law and as directed by the President.

(c) APPLICATION OF MORE STRINGENT STANDARDS.—The head of an agency may employ standards for the cost-effective information security for all operations and assets within or under the supervision of that agency that are more

stringent than the standards promulgated by the Director under this section, if such standards—

- (1) contain, at a minimum, the provisions of those applicable standards made compulsory and binding by the Director; and
- (2) are otherwise consistent with policies and guidelines issued under section 3533 of title 44.

(d) REQUIREMENTS REGARDING DECISIONS BY DIRECTOR.—

(1) DEADLINE.—The decision regarding the promulgation of any standard by the Director under subsection (b) shall occur not later than 6 months after the submission of the proposed standard to the Director by the National Institute of Standards and Technology, as provided under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g-3).

(2) NOTICE AND COMMENT.—A decision by the Director to significantly modify, or not promulgate a proposed standard submitted to the Director by the National Institute of Standards and Technology, as provided under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g-3), shall be made after the public is given an opportunity to comment on the Director's proposed decision.

CYBERSECURITY ACT OF 2015^[1]

[Division N of the Consolidated Appropriations Act of 2016]
[Public Law 114-113; 129 STAT. 2242; December 18, 2015]

SHORT TITLE; TABLE OF CONTENTS

SEC. 1.

(a) SHORT TITLE.—This division may be cited as the “Cybersecurity Act of 2015”.

(b) TABLE OF CONTENTS.—The table of contents for this division is as follows:

SEC. 1. Short title; table of contents.

TITLE I—CYBERSECURITY INFORMATION SHARING

SEC. 101. Short title.

SEC. 102. Definitions.

SEC. 103. Sharing of information by the Federal Government.

SEC. 104. Authorizations for preventing, detecting, analyzing, and mitigating cybersecurity threats.

SEC. 105. Sharing of cyber threat indicators and defensive measures with the Federal Government.

SEC. 106. Protection from liability.

SEC. 107. Oversight of Government activities.

SEC. 108. Construction and preemption.

SEC. 109. Report on cybersecurity threats.

SEC. 110. Exception to limitation on authority of Secretary of Defense to disseminate certain information.

SEC. 111. Effective period.

TITLE II—NATIONAL CYBERSECURITY ADVANCEMENT

SUBTITLE B—FEDERAL CYBERSECURITY ENHANCEMENT

SEC. 228. Identification of information systems relating to national security.

¹ Only select provisions are included, as reflected in the table of contents excerpt.

TITLE III—FEDERAL CYBERSECURITY WORKFORCE ASSESSMENT

- SEC. 301. Short title.
- SEC. 302. Definitions.
- SEC. 303. National cybersecurity workforce measurement initiative.
- SEC. 304. Identification of cyber-related work roles of critical need.
- SEC. 305. Government Accountability Office status reports.

TITLE IV—OTHER CYBER MATTERS

- SEC. 406. Federal computer security.

TITLE I—CYBERSECURITY INFORMATION SHARING

SHORT TITLE

- SEC. 101.
This title may be cited as the “Cybersecurity Information Sharing Act of 2015”.

DEFINITIONS

- SEC. 102. [6 U.S.C. § 1501]

In this title:

- (1) AGENCY.—The term “agency” has the meaning given the term in section 3502 of title 44, United States Code.
- (2) ANTITRUST LAWS.—The term “antitrust laws”—
 - (A) has the meaning given the term in the first section of the Clayton Act (15 U.S.C. 12);
 - (B) includes section 5 of the Federal Trade Commission Act (15 U.S.C. 45) to the extent that section 5 of that Act applies to unfair methods of competition; and
 - (C) includes any State antitrust law, but only to the extent that such law is consistent with the law referred to in subparagraph (A) or the law referred to in subparagraph (B).
- (3) APPROPRIATE FEDERAL ENTITIES.—The term “appropriate Federal entities” means the following:
 - (A) The Department of Commerce.
 - (B) The Department of Defense.
 - (C) The Department of Energy.
 - (D) The Department of Homeland Security.

(E) The Department of Justice.

(F) The Department of the Treasury.

(G) The Office of the Director of National Intelligence.

(4) **CYBERSECURITY PURPOSE.**—The term “cybersecurity purpose” means the purpose of protecting an information system or information that is stored on, processed by, or transiting an information system from a cybersecurity threat or security vulnerability.

(5) **CYBERSECURITY THREAT.**—

(A) **IN GENERAL.**—Except as provided in subparagraph (B), the term “cybersecurity threat” means an action, not protected by the First Amendment to the Constitution of the United States, on or through an information system that may result in an unauthorized effort to adversely impact the security, availability, confidentiality, or integrity of an information system or information that is stored on, processed by, or transiting an information system.

(B) **EXCLUSION.**—The term “cybersecurity threat” does not include any action that solely involves a violation of a consumer term of service or a consumer licensing agreement.

(6) **CYBER THREAT INDICATOR.**—The term “cyber threat indicator” means information that is necessary to describe or identify—

(A) malicious reconnaissance, including anomalous patterns of communications that appear to be transmitted for the purpose of gathering technical information related to a cybersecurity threat or security vulnerability;

(B) a method of defeating a security control or exploitation of a security vulnerability;

(C) a security vulnerability, including anomalous activity that appears to indicate the existence of a security vulnerability;

(D) a method of causing a user with legitimate access to an information system or information that is stored on, processed by, or transiting an information system to unwittingly enable the defeat of a security control or exploitation of a security vulnerability;

(E) malicious cyber command and control;

(F) the actual or potential harm caused by an incident, including a description of the information exfiltrated as a result of a particular cybersecurity threat;

(G) any other attribute of a cybersecurity threat, if disclosure of such attribute is not otherwise prohibited by law; or

(H) any combination thereof.

(7) **DEFENSIVE MEASURE.**—

(A) **IN GENERAL.**—Except as provided in subparagraph (B), the term “defensive measure” means an action, device, procedure, signature, technique, or other measure applied to an information system or information that is stored on, processed by, or transiting an information system that detects, prevents, or mitigates a known or suspected cybersecurity threat or security vulnerability.

(B) **EXCLUSION.**—The term “defensive measure” does not include a measure that destroys, renders unusable, provides unauthorized access to, or substantially harms an information system or information stored on, processed by, or transiting such information system not owned by—

(i) the private entity operating the measure; or

(ii) another entity or Federal entity that is authorized to provide consent and has provided consent to that private entity for operation of such measure.

(8) **FEDERAL ENTITY.**—The term “Federal entity” means a department or agency of the United States or any component of such department or agency.

(9) **INFORMATION SYSTEM.**—The term “information system”—

(A) has the meaning given the term in section 3502 of title 44, United States Code; and

(B) includes industrial control systems, such as supervisory control and data acquisition systems, distributed control systems, and programmable logic controllers.

(10) **LOCAL GOVERNMENT.**—The term “local government” means any borough, city, county, parish, town, township, village, or other political subdivision of a State.

(11) **MALICIOUS CYBER COMMAND AND CONTROL.**—The term “malicious cyber command and control” means a method for unauthorized remote identification of, access to, or use of, an information system or information that is stored on, processed by, or transiting an information system.

(12) **MALICIOUS RECONNAISSANCE.**—The term “malicious reconnaissance” means a method for actively probing or passively monitoring an information system for the purpose of discerning security vulnerabilities of the information system, if such method is associated with a known or suspected cybersecurity threat.

(13) **MONITOR.**—The term “monitor” means to acquire, identify, or scan, or to possess, information that is stored on, processed by, or transiting an information system.

(14) **NON-FEDERAL ENTITY.**—

(A) **IN GENERAL.**—Except as otherwise provided in this paragraph, the term “non-Federal entity” means any private entity, non-Federal

government agency or department, or State, tribal, or local government (including a political subdivision, department, or component thereof).

(B) INCLUSIONS.—The term “non-Federal entity” includes a government agency or department of the District of Columbia, the Commonwealth of Puerto Rico, the United States Virgin Islands, Guam, American Samoa, the Northern Mariana Islands, and any other territory or possession of the United States.

(C) EXCLUSION.—The term “non-Federal entity” does not include a foreign power as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801).

(15) PRIVATE ENTITY.—

(A) IN GENERAL.—Except as otherwise provided in this paragraph, the term “private entity” means any person or private group, organization, proprietorship, partnership, trust, cooperative, corporation, or other commercial or nonprofit entity, including an officer, employee, or agent thereof.

(B) INCLUSION.—The term “private entity” includes a State, tribal, or local government performing utility services, such as electric, natural gas, or water services.

(C) EXCLUSION.—The term “private entity” does not include a foreign power as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801).

(16) SECURITY CONTROL.—The term “security control” means the management, operational, and technical controls used to protect against an unauthorized effort to adversely affect the confidentiality, integrity, and availability of an information system or its information.

(17) SECURITY VULNERABILITY.—The term “security vulnerability” means any attribute of hardware, software, process, or procedure that could enable or facilitate the defeat of a security control.

(18) TRIBAL.—The term “tribal” has the meaning given the term “Indian tribe” in section 4 of the Indian Self-Determination and Education Assistance Act (25 U.S.C. 450b).

SHARING OF INFORMATION BY THE FEDERAL GOVERNMENT

SEC. 103. [6 U.S.C. § 1502]

(a) IN GENERAL.—Consistent with the protection of classified information, intelligence sources and methods, and privacy and civil liberties, the Director of National Intelligence, the Secretary of Homeland Security, the Secretary of Defense, and the Attorney General, in consultation with the heads of the

appropriate Federal entities, shall jointly develop and issue procedures to facilitate and promote—

- (1) the timely sharing of classified cyber threat indicators and defensive measures in the possession of the Federal Government with representatives of relevant Federal entities and non-Federal entities that have appropriate security clearances;
- (2) the timely sharing with relevant Federal entities and non-Federal entities of cyber threat indicators, defensive measures, and information relating to cybersecurity threats or authorized uses under this title, in the possession of the Federal Government that may be declassified and shared at an unclassified level;
- (3) the timely sharing with relevant Federal entities and non-Federal entities, or the public if appropriate, of unclassified, including controlled unclassified, cyber threat indicators and defensive measures in the possession of the Federal Government;
- (4) the timely sharing with Federal entities and non-Federal entities, if appropriate, of information relating to cybersecurity threats or authorized uses under this title, in the possession of the Federal Government about cybersecurity threats to such entities to prevent or mitigate adverse effects from such cybersecurity threats; and
- (5) the periodic sharing, through publication and targeted outreach, of cybersecurity best practices that are developed based on ongoing analyses of cyber threat indicators, defensive measures, and information relating to cybersecurity threats or authorized uses under this title, in the possession of the Federal Government, with attention to accessibility and implementation challenges faced by small business concerns (as defined in section 3 of the Small Business Act (15 U.S.C. 632)).

(b) DEVELOPMENT OF PROCEDURES.—

(1) IN GENERAL.—The procedures developed under subsection (a) shall—

- (A) ensure the Federal Government has and maintains the capability to share cyber threat indicators and defensive measures in real time consistent with the protection of classified information;
- (B) incorporate, to the greatest extent practicable, existing processes and existing roles and responsibilities of Federal entities and non-Federal entities for information sharing by the Federal Government, including sector specific information sharing and analysis centers;
- (C) include procedures for notifying, in a timely manner, Federal entities and non-Federal entities that have received a cyber threat

indicator or defensive measure from a Federal entity under this title that is known or determined to be in error or in contravention of the requirements of this title or another provision of Federal law or policy of such error or contravention; (D) include requirements for Federal entities sharing cyber threat indicators or defensive measures to implement and utilize security controls to protect against unauthorized access to or acquisition of such cyber threat indicators or defensive measures; (E) include procedures that require a Federal entity, prior to the sharing of a cyber threat indicator—

(i) to review such cyber threat indicator to assess whether such cyber threat indicator contains any information not directly related to a cybersecurity threat that such Federal entity knows at the time of sharing to be personal information of a specific individual or information that identifies a specific individual and remove such information; or

(ii) to implement and utilize a technical capability configured to remove any information not directly related to a cybersecurity threat that the Federal entity knows at the time of sharing to be personal information of a specific individual or information that identifies a specific individual; and

(F) include procedures for notifying, in a timely manner, any United States person whose personal information is known or determined to have been shared by a Federal entity in violation of this title.

(2) CONSULTATION.—In developing the procedures required under this section, the Director of National Intelligence, the Secretary of Homeland Security, the Secretary of Defense, and the Attorney General shall consult with appropriate Federal entities, including the Small Business Administration and the National Laboratories (as defined in section 2 of the Energy Policy Act of 2005 (42 U.S.C. 15801)), to ensure that effective protocols are implemented that will facilitate and promote the sharing of cyber threat indicators by the Federal Government in a timely manner.

(c) SUBMITTAL TO CONGRESS.—Not later than 60 days after the date of the enactment of this Act, the Director of National Intelligence, in consultation with the heads of the appropriate Federal entities, shall submit to Congress the procedures required by subsection (a).

**AUTHORIZATIONS FOR PREVENTING, DETECTING, ANALYZING, AND
MITIGATING CYBERSECURITY THREATS**

SEC. 104. [6 U.S.C. § 1503]

(a) AUTHORIZATION FOR MONITORING.—

(1) IN GENERAL.—Notwithstanding any other provision of law, a private entity may, for cybersecurity purposes, monitor—

- (A) an information system of such private entity;
- (B) an information system of another non-Federal entity, upon the authorization and written consent of such other entity;
- (C) an information system of a Federal entity, upon the authorization and written consent of an authorized representative of the Federal entity; and
- (D) information that is stored on, processed by, or transiting an information system monitored by the private entity under this paragraph.

(2) CONSTRUCTION.—Nothing in this subsection shall be construed—

- (A) to authorize the monitoring of an information system, or the use of any information obtained through such monitoring, other than as provided in this title; or
- (B) to limit otherwise lawful activity.

(b) AUTHORIZATION FOR OPERATION OF DEFENSIVE MEASURES.—

(1) IN GENERAL.—Notwithstanding any other provision of law, a private entity may, for cybersecurity purposes, operate a defensive measure that is applied to—

- (A) an information system of such private entity in order to protect the rights or property of the private entity;
- (B) an information system of another non-Federal entity upon written consent of such entity for operation of such defensive measure to protect the rights or property of such entity; and
- (C) an information system of a Federal entity upon written consent of an authorized representative of such Federal entity for operation of such defensive measure to protect the rights or property of the Federal Government.

(2) CONSTRUCTION.—Nothing in this subsection shall be construed—

- (A) to authorize the use of a defensive measure other than as provided in this subsection; or
- (B) to limit otherwise lawful activity.

(c) AUTHORIZATION FOR SHARING OR RECEIVING CYBER THREAT INDICATORS OR DEFENSIVE MEASURES.—

(1) IN GENERAL.—Except as provided in paragraph (2) and notwithstanding any other provision of law, a non-Federal entity may, for a cybersecurity purpose and consistent with the protection of classified information, share with, or receive from, any other non-Federal entity or the Federal Government a cyber threat indicator or defensive measure.

(2) LAWFUL RESTRICTION.—A non-Federal entity receiving a cyber threat indicator or defensive measure from another non-Federal entity or a Federal entity shall comply with otherwise lawful restrictions placed on the sharing or use of such cyber threat indicator or defensive measure by the sharing non-Federal entity or Federal entity.

(3) CONSTRUCTION.—Nothing in this subsection shall be construed—

(A) to authorize the sharing or receiving of a cyber threat indicator or defensive measure other than as provided in this subsection; or

(B) to limit otherwise lawful activity.

(d) PROTECTION AND USE OF INFORMATION.—

(1) SECURITY OF INFORMATION.—A non-Federal entity monitoring an information system, operating a defensive measure, or providing or receiving a cyber threat indicator or defensive measure under this section shall implement and utilize a security control to protect against unauthorized access to or acquisition of such cyber threat indicator or defensive measure.

(2) REMOVAL OF CERTAIN PERSONAL INFORMATION.—A non-Federal entity sharing a cyber threat indicator pursuant to this title shall, prior to such sharing—

(A) review such cyber threat indicator to assess whether such cyber threat indicator contains any information not directly related to a cybersecurity threat that the non-Federal entity knows at the time of sharing to be personal information of a specific individual or information that identifies a specific individual and remove such information; or

(B) implement and utilize a technical capability configured to remove any information not directly related to a cybersecurity threat that the non-Federal entity knows at the time of sharing to be personal information of a specific individual or information that identifies a specific individual.

(3) USE OF CYBER THREAT INDICATORS AND DEFENSIVE MEASURES BY NON-FEDERAL ENTITIES.—

(A) IN GENERAL.—Consistent with this title, a cyber threat indicator or defensive measure shared or received under this section may, for cybersecurity purposes—

(i) be used by a non-Federal entity to monitor or operate a defensive measure that is applied to—

(I) an information system of the non-Federal entity; or

(II) an information system of another non-Federal entity or a Federal entity upon the written consent of that other non-Federal entity or that Federal entity; and

(ii) be otherwise used, retained, and further shared by a non-Federal entity subject to—

(I) an otherwise lawful restriction placed by the sharing non-Federal entity or Federal entity on such cyber threat indicator or defensive measure; or

(II) an otherwise applicable provision of law.

(B) CONSTRUCTION.—Nothing in this paragraph shall be construed to authorize the use of a cyber threat indicator or defensive measure other than as provided in this section.

(4) USE OF CYBER THREAT INDICATORS BY STATE, TRIBAL, OR LOCAL GOVERNMENT.—

(A) LAW ENFORCEMENT USE.—A State, tribal, or local government that receives a cyber threat indicator or defensive measure under this title may use such cyber threat indicator or defensive measure for the purposes described in section 105(d)(5)(A).

(B) EXEMPTION FROM DISCLOSURE.—A cyber threat indicator or defensive measure shared by or with a State, tribal, or local government, including a component of a State, tribal, or local government that is a private entity, under this section shall be—

(i) deemed voluntarily shared information; and

(ii) exempt from disclosure under any provision of State, tribal, or local freedom of information law, open government law, open meetings law, open records law, sunshine law, or similar law requiring disclosure of information or records.

(C) STATE, TRIBAL, AND LOCAL REGULATORY AUTHORITY.—

(i) IN GENERAL.—Except as provided in clause (ii), a cyber threat indicator or defensive measure shared with a State, tribal, or local government under this title shall not be used by any State, tribal, or local government to regulate, including an enforcement action, the lawful activity of any non-Federal entity or any activity taken by a non-Federal entity pursuant to mandatory standards, including an activity relating to monitoring, operating a defensive measure, or sharing of a cyber threat indicator.

(ii) REGULATORY AUTHORITY SPECIFICALLY RELATING TO PREVENTION OR MITIGATION OF CYBERSECURITY THREATS.—A cyber threat indicator or defensive measure shared as described in clause (i) may, consistent with a State, tribal, or local government regulatory authority specifically relating to the prevention or mitigation of cybersecurity threats to information systems, inform the development or implementation of a regulation relating to such information systems.

(e) ANTITRUST EXEMPTION.—

(1) IN GENERAL.—Except as provided in section 108(e), it shall not be considered a violation of any provision of antitrust laws for 2 or more private entities to exchange or provide a cyber threat indicator or defensive measure, or assistance relating to the prevention, investigation, or mitigation of a cybersecurity threat, for cybersecurity purposes under this title.

(2) APPLICABILITY.—Paragraph (1) shall apply only to information that is exchanged or assistance provided in order to assist with—

(A) facilitating the prevention, investigation, or mitigation of a cybersecurity threat to an information system or information that is stored on, processed by, or transiting an information system;
or

(B) communicating or disclosing a cyber threat indicator to help prevent, investigate, or mitigate the effect of a cybersecurity threat to an information system or information that is stored on, processed by, or transiting an information system.

(f) NO RIGHT OR BENEFIT.—The sharing of a cyber threat indicator or defensive measure with a non-Federal entity under this title shall not create a right or benefit to similar information by such non-Federal entity or any other non-Federal entity.

**SHARING OF CYBER THREAT INDICATORS AND DEFENSIVE MEASURES WITH
THE FEDERAL GOVERNMENT**

SEC. 105. [6 U.S.C. § 1504]

(a) REQUIREMENT FOR POLICIES AND PROCEDURES.—

(1) INTERIM POLICIES AND PROCEDURES.—Not later than 60 days after the date of the enactment of this Act, the Attorney General and the Secretary of Homeland Security shall, in consultation with the heads of the appropriate Federal entities, jointly develop and submit to Congress interim policies and procedures relating to the receipt of cyber threat indicators and defensive measures by the Federal Government.

(2) FINAL POLICIES AND PROCEDURES.—Not later than 180 days after the date of the enactment of this Act, the Attorney General and the Secretary of Homeland Security shall, in consultation with the heads of the appropriate Federal entities, jointly issue and make publicly available final policies and procedures relating to the receipt of cyber threat indicators and defensive measures by the Federal Government.

(3) REQUIREMENTS CONCERNING POLICIES AND PROCEDURES.—Consistent with the guidelines required by subsection (b), the policies and procedures developed or issued under this subsection shall—

(A) ensure that cyber threat indicators shared with the Federal Government by any non-Federal entity pursuant to section 104(c) through the real-time process described in subsection (c) of this section—

- (i) are shared in an automated manner with all of the appropriate Federal entities;
- (ii) are only subject to a delay, modification, or other action due to controls established for such real-time process that could impede real-time receipt by all of the appropriate Federal entities when the delay, modification, or other action is due to controls—

(I) agreed upon unanimously by all of the heads of the appropriate Federal entities;

(II) carried out before any of the appropriate Federal entities retains or uses the cyber threat indicators or defensive measures; and

(III) uniformly applied such that each of the appropriate Federal entities is subject to the same delay, modification, or other action; and

(iii) may be provided to other Federal entities;

(B) ensure that cyber threat indicators shared with the Federal Government by any non-Federal entity pursuant to section 104 in a manner other than the real-time process described in subsection (c) of this section—

- (i) are shared as quickly as operationally practicable with all of the appropriate Federal entities;
- (ii) are not subject to any unnecessary delay, interference, or any other action that could impede receipt by all of the appropriate Federal entities; and
- (iii) may be provided to other Federal entities; and

(C) ensure there are—

- (i) audit capabilities; and
- (ii) appropriate sanctions in place for officers, employees, or agents of a Federal entity who knowingly and willfully conduct activities under this title in an unauthorized manner.

(4) GUIDELINES FOR ENTITIES SHARING CYBER THREAT INDICATORS WITH FEDERAL GOVERNMENT.—

(A) **IN GENERAL.**—Not later than 60 days after the date of the enactment of this Act, the Attorney General and the Secretary of Homeland Security shall jointly develop and make publicly available guidance to assist entities and promote sharing of cyber threat indicators with Federal entities under this title.

(B) **CONTENTS.**—The guidelines developed and made publicly available under subparagraph (A) shall include guidance on the following:

(i) Identification of types of information that would qualify as a cyber threat indicator under this title that would be unlikely to include information that—

- (I) is not directly related to a cybersecurity threat; and
- (II) is personal information of a specific individual or information that identifies a specific individual.

(ii) Identification of types of information protected under otherwise applicable privacy laws that are unlikely to be directly related to a cybersecurity threat.

(iii) Such other matters as the Attorney General and the Secretary of Homeland Security consider appropriate for entities sharing cyber threat indicators with Federal entities under this title.

(b) PRIVACY AND CIVIL LIBERTIES.—

(1) INTERIM GUIDELINES.—Not later than 60 days after the date of the enactment of this Act, the Attorney General and the Secretary of Homeland Security shall, in consultation with heads of the appropriate Federal entities and in consultation with officers designated under section 1062 of the National Security Intelligence Reform Act of 2004 (42 U.S.C. 2000ee–1), jointly develop, submit to Congress, and make available to the public interim guidelines relating to privacy and civil liberties which shall govern the receipt, retention, use, and dissemination of cyber threat indicators by a Federal entity obtained in connection with activities authorized in this title.

(2) FINAL GUIDELINES.—

(A) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Attorney General and the Secretary of Homeland Security shall, in coordination with heads of the appropriate Federal entities and in consultation with officers designated under section 1062 of the National Security Intelligence Reform Act of 2004 (42 U.S.C. 2000ee–1) and such private entities with industry expertise as the Attorney General and the Secretary consider relevant, jointly issue and make publicly available final guidelines relating to privacy and civil liberties which shall govern the receipt, retention, use, and dissemination of cyber threat indicators by a Federal entity obtained in connection with activities authorized in this title.

(B) PERIODIC REVIEW.—The Attorney General and the Secretary of Homeland Security shall, in coordination with heads of the appropriate Federal entities and in consultation with officers and private entities described in subparagraph (A), periodically, but not less frequently than once every 2 years, jointly review the guidelines issued under subparagraph (A).

(3) CONTENT.—The guidelines required by paragraphs (1) and (2) shall, consistent with the need to protect information systems from cybersecurity threats and mitigate cybersecurity threats—

(A) limit the effect on privacy and civil liberties of activities by the Federal Government under this title;

(B) limit the receipt, retention, use, and dissemination of cyber threat indicators containing personal information of specific individuals or information that identifies specific individuals, including by establishing—

(i) a process for the timely destruction of such information that is known not to be directly related to uses authorized under this title; and

(ii) specific limitations on the length of any period in which a cyber threat indicator may be retained;

(C) include requirements to safeguard cyber threat indicators containing personal information of specific individuals or information that identifies specific individuals from unauthorized access or acquisition, including appropriate sanctions for activities by officers, employees, or agents of the Federal Government in contravention of such guidelines;

(D) consistent with this title, any other applicable provisions of law, and the fair information practice principles set forth in appendix A of the document entitled “National Strategy for Trusted Identities in Cyberspace” and published by the President in April 2011, govern the retention, use, and dissemination by the Federal Government of cyber threat indicators shared with the Federal Government under this title, including the extent, if any, to which such cyber threat indicators may be used by the Federal Government;

(E) include procedures for notifying entities and Federal entities if information received pursuant to this section is known or determined by a Federal entity receiving such information not to constitute a cyber threat indicator;

(F) protect the confidentiality of cyber threat indicators containing personal information of specific individuals or information that identifies specific individuals to the greatest extent practicable and require recipients to be informed that such indicators may only be used for purposes authorized under this title; and

(G) include steps that may be needed so that dissemination of cyber threat indicators is consistent with the protection of classified and other sensitive national security information.

(c) CAPABILITY AND PROCESS WITHIN THE DEPARTMENT OF HOMELAND SECURITY.—

(1) **IN GENERAL.**—Not later than 90 days after the date of the enactment of this Act, the Secretary of Homeland Security, in coordination with the heads of the appropriate Federal entities, shall develop and implement a capability and process within the Department of Homeland Security that—

- (A) shall accept from any non-Federal entity in real time cyber threat indicators and defensive measures, pursuant to this section;
- (B) shall, upon submittal of the certification under paragraph (2) that such capability and process fully and effectively operates as described in such paragraph, be the process by which the Federal Government receives cyber threat indicators and defensive measures under this title that are shared by a non-Federal entity with the Federal Government through electronic mail or media, an interactive form on an Internet website, or a real time, automated process between information systems except—
- (i) consistent with section 104, communications between a Federal entity and a non-Federal entity regarding a previously shared cyber threat indicator to describe the relevant cybersecurity threat or develop a defensive measure based on such cyber threat indicator; and
 - (ii) communications by a regulated non-Federal entity with such entity's Federal regulatory authority regarding a cybersecurity threat;
- (C) ensures that all of the appropriate Federal entities receive in an automated manner such cyber threat indicators and defensive measures shared through the real-time process within the Department of Homeland Security;
- (D) is in compliance with the policies, procedures, and guidelines required by this section; and
- (E) does not limit or prohibit otherwise lawful disclosures of communications, records, or other information, including—
- (i) reporting of known or suspected criminal activity, by a non-Federal entity to any other non-Federal entity or a Federal entity, including cyber threat indicators or defensive measures shared with a Federal entity in furtherance of opening a Federal law enforcement investigation;
 - (ii) voluntary or legally compelled participation in a Federal investigation; and
 - (iii) providing cyber threat indicators or defensive measures as part of a statutory or authorized contractual requirement.

(2) CERTIFICATION AND DESIGNATION.—

- (A) CERTIFICATION OF CAPABILITY AND PROCESS.—Not later than 90 days after the date of the enactment of this Act, the

Secretary of Homeland Security shall, in consultation with the heads of the appropriate Federal entities, submit to Congress a certification as to whether the capability and process required by paragraph (1) fully and effectively operates—

- (i) as the process by which the Federal Government receives from any non-Federal entity a cyber threat indicator or defensive measure under this title; and
- (ii) in accordance with the interim policies, procedures, and guidelines developed under this title.

(B) DESIGNATION.—

(i) IN GENERAL.—At any time after certification is submitted under subparagraph (A), the President may designate an appropriate Federal entity, other than the Department of Defense (including the National Security Agency), to develop and implement a capability and process as described in paragraph (1) in addition to the capability and process developed under such paragraph by the Secretary of Homeland Security, if, not fewer than 30 days before making such designation, the President submits to Congress a certification and explanation that—

- (I) such designation is necessary to ensure that full, effective, and secure operation of a capability and process for the Federal Government to receive from any non-Federal entity cyber threat indicators or defensive measures under this title;
- (II) the designated appropriate Federal entity will receive and share cyber threat indicators and defensive measures in accordance with the policies, procedures, and guidelines developed under this title, including subsection (a)(3)(A); and
- (III) such designation is consistent with the mission of such appropriate Federal entity and improves the ability of the Federal Government to receive, share, and use cyber threat indicators and defensive measures as authorized under this title.

(ii) Application to Additional Capability and Process.—If the President designates an appropriate Federal entity

to develop and implement a capability and process under clause (i), the provisions of this title that apply to the capability and process required by paragraph (1) shall also be construed to apply to the capability and process developed and implemented under clause (i).

(3) PUBLIC NOTICE AND ACCESS.—The Secretary of Homeland Security shall ensure there is public notice of, and access to, the capability and process developed and implemented under paragraph (1) so that—

(A) any non-Federal entity may share cyber threat indicators and defensive measures through such process with the Federal Government; and

(B) all of the appropriate Federal entities receive such cyber threat indicators and defensive measures in real time with receipt through the process within the Department of Homeland Security consistent with the policies and procedures issued under subsection (a).

(4) OTHER FEDERAL ENTITIES.—The process developed and implemented under paragraph (1) shall ensure that other Federal entities receive in a timely manner any cyber threat indicators and defensive measures shared with the Federal Government through such process.

(d) INFORMATION SHARED WITH OR PROVIDED TO THE FEDERAL GOVERNMENT.—

(1) NO WAIVER OF PRIVILEGE OR PROTECTION.—The provision of cyber threat indicators and defensive measures to the Federal Government under this title shall not constitute a waiver of any applicable privilege or protection provided by law, including trade secret protection.

(2) PROPRIETARY INFORMATION.—Consistent with section 104(c)(2) and any other applicable provision of law, a cyber threat indicator or defensive measure provided by a non-Federal entity to the Federal Government under this title shall be considered the commercial, financial, and proprietary information of such non-Federal entity when so designated by the originating non-Federal entity or a third party acting in accordance with the written authorization of the originating non-Federal entity.

(3) EXEMPTION FROM DISCLOSURE.—A cyber threat indicator or defensive measure shared with the Federal Government under this title shall be—

(A) deemed voluntarily shared information and exempt from disclosure under section 552 of title 5, United States Code, and any State, tribal, or local provision of law requiring disclosure of information or records; and

(B) withheld, without discretion, from the public under section 552(b)(3)(B) of title 5, United States Code, and any State, tribal, or local provision of law requiring disclosure of information or records.

(4) EX PARTE COMMUNICATIONS.—The provision of a cyber threat indicator or defensive measure to the Federal Government under this title shall not be subject to a rule of any Federal agency or department or any judicial doctrine regarding ex parte communications with a decision-making official.

(5) DISCLOSURE, RETENTION, AND USE.—

(A) AUTHORIZED ACTIVITIES.—Cyber threat indicators and defensive measures provided to the Federal Government under this title may be disclosed to, retained by, and used by, consistent with otherwise applicable provisions of Federal law, any Federal agency or department, component, officer, employee, or agent of the Federal Government solely for—

(i) a cybersecurity purpose;

(ii) the purpose of identifying—

(I) a cybersecurity threat, including the source of such cybersecurity threat; or

(II) a security vulnerability;

(iii) the purpose of responding to, or otherwise preventing or mitigating, a specific threat of death, a specific threat of serious bodily harm, or a specific threat of serious economic harm, including a terrorist act or a use of a weapon of mass destruction;

(iv) the purpose of responding to, investigating, prosecuting, or otherwise preventing or mitigating, a serious threat to a minor, including sexual exploitation and threats to physical safety; or

(v) the purpose of preventing, investigating, disrupting, or prosecuting an offense arising out of a threat described in clause (iii) or any of the offenses listed in—

(I) sections 1028 through 1030 of title 18, United States Code (relating to fraud and identity theft);

(II) chapter 37 of such title (relating to espionage and censorship); and

(III) chapter 90 of such title (relating to protection of trade secrets).

(B) PROHIBITED ACTIVITIES.—Cyber threat indicators and defensive measures provided to the Federal Government under this title shall not be disclosed to, retained by, or used by any Federal agency or department for any use not permitted under subparagraph (A).

(C) PRIVACY AND CIVIL LIBERTIES.—Cyber threat indicators and defensive measures provided to the Federal Government under this title shall be retained, used, and disseminated by the Federal Government—

(i) in accordance with the policies, procedures, and guidelines required by subsections (a) and (b);

(ii) in a manner that protects from unauthorized use or disclosure any cyber threat indicators that may contain—

(I) personal information of a specific individual;

or

(II) information that identifies a specific individual; and

(iii) in a manner that protects the confidentiality of cyber threat indicators containing—

(I) personal information of a specific individual;

or

(II) information that identifies a specific individual.

(D) FEDERAL REGULATORY AUTHORITY.—

(i) IN GENERAL.—Except as provided in clause (ii), cyber threat indicators and defensive measures provided to the Federal Government under this title shall not be used by any Federal, State, tribal, or local government to regulate, including an enforcement action, the lawful activities of any non-Federal entity or any activities taken by a non-Federal entity pursuant to mandatory standards, including activities relating to monitoring, operating defensive measures, or sharing cyber threat indicators.

(ii) EXCEPTIONS.—

(I) REGULATORY AUTHORITY SPECIFICALLY RELATING TO PREVENTION OR MITIGATION OF CYBERSECURITY THREATS.—Cyber threat indicators and defensive measures provided to the Federal Government under this title may, consistent with Federal or State regulatory

authority specifically relating to the prevention or mitigation of cybersecurity threats to information systems, inform the development or implementation of regulations relating to such information systems.

(II) PROCEDURES DEVELOPED AND IMPLEMENTED UNDER THIS TITLE.—Clause (i) shall not apply to procedures developed and implemented under this title.

PROTECTION FROM LIABILITY

SEC. 106. [6 U.S.C. § 1505]

(a) **MONITORING OF INFORMATION SYSTEMS.**—No cause of action shall lie or be maintained in any court against any private entity, and such action shall be promptly dismissed, for the monitoring of an information system and information under section 104(a) that is conducted in accordance with this title.

(b) **SHARING OR RECEIPT OF CYBER THREAT INDICATORS.**—No cause of action shall lie or be maintained in any court against any private entity, and such action shall be promptly dismissed, for the sharing or receipt of a cyber threat indicator or defensive measure under section 104(c) if—

- (1) such sharing or receipt is conducted in accordance with this title; and
- (2) in a case in which a cyber threat indicator or defensive measure is shared with the Federal Government, the cyber threat indicator or defensive measure is shared in a manner that is consistent with section 105(c)(1)(B) and the sharing or receipt, as the case may be, occurs after the earlier of—

(A) the date on which the interim policies and procedures are submitted to Congress under section 105(a)(1) and guidelines are submitted to Congress under section 105(b)(1); or

(B) the date that is 60 days after the date of the enactment of this Act.

(c) **CONSTRUCTION.**—Nothing in this title shall be construed—

- (1) to create—

(A) a duty to share a cyber threat indicator or defensive measure; or

(B) a duty to warn or act based on the receipt of a cyber threat indicator or defensive measure; or

- (2) to undermine or limit the availability of otherwise applicable common law or statutory defenses.

OVERSIGHT OF GOVERNMENT ACTIVITIES

SEC. 107. [6 U.S.C. § 1506]

(a) REPORT ON IMPLEMENTATION.—

(1) IN GENERAL.—Not later than 1 year after the date of the enactment of this title, the heads of the appropriate Federal entities shall jointly submit to Congress a detailed report concerning the implementation of this title.

(2) CONTENTS.—The report required by paragraph (1) may include such recommendations as the heads of the appropriate Federal entities may have for improvements or modifications to the authorities, policies, procedures, and guidelines under this title and shall include the following:

(A) An evaluation of the effectiveness of real-time information sharing through the capability and process developed under section 105(c), including any impediments to such real-time sharing.

(B) An assessment of whether cyber threat indicators or defensive measures have been properly classified and an accounting of the number of security clearances authorized by the Federal Government for the purpose of sharing cyber threat indicators or defensive measures with the private sector.

(C) The number of cyber threat indicators or defensive measures received through the capability and process developed under section 105(c).

(D) A list of Federal entities that have received cyber threat indicators or defensive measures under this title.

(b) BIENNIAL REPORT ON COMPLIANCE.—

(1) IN GENERAL.—Not later than 2 years after the date of the enactment of this Act and not less frequently than once every 2 years thereafter, the inspectors general of the appropriate Federal entities, in consultation with the Inspector General of the Intelligence Community and the Council of Inspectors General on Financial Oversight, shall jointly submit to Congress an interagency report on the actions of the executive branch of the Federal Government to carry out this title during the most recent 2-year period.

(2) CONTENTS.—Each report submitted under paragraph (1) shall include, for the period covered by the report, the following:

(A) An assessment of the sufficiency of the policies, procedures, and guidelines relating to the sharing of cyber threat indicators within the Federal Government, including those policies, procedures, and guidelines relating to the removal of information

not directly related to a cybersecurity threat that is personal information of a specific individual or information that identifies a specific individual.

(B) An assessment of whether cyber threat indicators or defensive measures have been properly classified and an accounting of the number of security clearances authorized by the Federal Government for the purpose of sharing cyber threat indicators or defensive measures with the private sector.

(C) A review of the actions taken by the Federal Government based on cyber threat indicators or defensive measures shared with the Federal Government under this title, including a review of the following:

(i) The appropriateness of subsequent uses and disseminations of cyber threat indicators or defensive measures.

(ii) Whether cyber threat indicators or defensive measures were shared in a timely and adequate manner with appropriate entities, or, if appropriate, were made publicly available.

(D) An assessment of the cyber threat indicators or defensive measures shared with the appropriate Federal entities under this title, including the following:

(i) The number of cyber threat indicators or defensive measures shared through the capability and process developed under section 105(c).

(ii) An assessment of any information not directly related to a cybersecurity threat that is personal information of a specific individual or information identifying a specific individual and was shared by a non-Federal government entity with the Federal government in contravention of this title, or was shared within the Federal Government in contravention of the guidelines required by this title, including a description of any significant violation of this title.

(iii) The number of times, according to the Attorney General, that information shared under this title was used by a Federal entity to prosecute an offense listed in section 105(d)(5)(A).

(iv) A quantitative and qualitative assessment of the effect of the sharing of cyber threat indicators or defensive measures with the Federal Government on

privacy and civil liberties of specific individuals, including the number of notices that were issued with respect to a failure to remove information not directly related to a cybersecurity threat that was personal information of a specific individual or information that identified a specific individual in accordance with the procedures required by section 105(b)(3)(E).

(v) The adequacy of any steps taken by the Federal Government to reduce any adverse effect from activities carried out under this title on the privacy and civil liberties of United States persons.

(E) An assessment of the sharing of cyber threat indicators or defensive measures among Federal entities to identify inappropriate barriers to sharing information.

(3) RECOMMENDATIONS.—Each report submitted under this subsection may include such recommendations as the inspectors general may have for improvements or modifications to the authorities and processes under this title.

(c) INDEPENDENT REPORT ON REMOVAL OF PERSONAL INFORMATION.—Not later than 3 years after the date of the enactment of this Act, the Comptroller General of the United States shall submit to Congress a report on the actions taken by the Federal Government to remove personal information from cyber threat indicators or defensive measures pursuant to this title. Such report shall include an assessment of the sufficiency of the policies, procedures, and guidelines established under this title in addressing concerns relating to privacy and civil liberties.

(d) FORM OF REPORTS.—Each report required under this section shall be submitted in an unclassified form, but may include a classified annex.

(e) PUBLIC AVAILABILITY OF REPORTS.—The unclassified portions of the reports required under this section shall be made available to the public.

CONSTRUCTION AND PREEMPTION

SEC. 108. [6 U.S.C. § 1507]

(a) OTHERWISE LAWFUL DISCLOSURES.—Nothing in this title shall be construed—

(1) to limit or prohibit otherwise lawful disclosures of communications, records, or other information, including reporting of known or suspected criminal activity, by a non-Federal entity to any other non-Federal entity or the Federal Government under this title; or

(2) to limit or prohibit otherwise lawful use of such disclosures by any Federal entity, even when such otherwise lawful disclosures duplicate or replicate disclosures made under this title.

(b) **WHISTLE BLOWER PROTECTIONS.**—Nothing in this title shall be construed to prohibit or limit the disclosure of information protected under section 2302(b)(8) of title 5, United States Code (governing disclosures of illegality, waste, fraud, abuse, or public health or safety threats), section 7211 of title 5, United States Code (governing disclosures to Congress), section 1034 of title 10, United States Code (governing disclosure to Congress by members of the military), section 1104 of the National Security Act of 1947 (50 U.S.C. 3234) (governing disclosure by employees of elements of the intelligence community), or any similar provision of Federal or State law.

(c) **PROTECTION OF SOURCES AND METHODS.**—Nothing in this title shall be construed—

(1) as creating any immunity against, or otherwise affecting, any action brought by the Federal Government, or any agency or department thereof, to enforce any law, executive order, or procedure governing the appropriate handling, disclosure, or use of classified information;

(2) to affect the conduct of authorized law enforcement or intelligence activities; or

(3) to modify the authority of a department or agency of the Federal Government to protect classified information and sources and methods and the national security of the United States.

(d) **RELATIONSHIP TO OTHER LAWS.**—Nothing in this title shall be construed to affect any requirement under any other provision of law for a non-Federal entity to provide information to the Federal Government.

(e) **PROHIBITED CONDUCT.**—Nothing in this title shall be construed to permit price-fixing, allocating a market between competitors, monopolizing or attempting to monopolize a market, boycotting, or exchanges of price or cost information, customer lists, or information regarding future competitive planning.

(f) **INFORMATION SHARING RELATIONSHIPS.**—Nothing in this title shall be construed—

(1) to limit or modify an existing information sharing relationship;

(2) to prohibit a new information sharing relationship;

(3) to require a new information sharing relationship between any non-Federal entity and a Federal entity or another non-Federal entity; or

(4) to require the use of the capability and process within the Department of Homeland Security developed under section 4105(c).

(g) PRESERVATION OF CONTRACTUAL OBLIGATIONS AND RIGHTS.—Nothing in this title shall be construed—

- (1) to amend, repeal, or supersede any current or future contractual agreement, terms of service agreement, or other contractual relationship between any non-Federal entities, or between any non-Federal entity and a Federal entity; or
- (2) to abrogate trade secret or intellectual property rights of any non-Federal entity or Federal entity.

(h) ANTI-TASKING RESTRICTION.—Nothing in this title shall be construed to permit a Federal entity—

- (1) to require a non-Federal entity to provide information to a Federal entity or another non-Federal entity;
- (2) to condition the sharing of cyber threat indicators with a non-Federal entity on such entity's provision of cyber threat indicators to a Federal entity or another non-Federal entity; or
- (3) to condition the award of any Federal grant, contract, or purchase on the provision of a cyber threat indicator to a Federal entity or another non-Federal entity.

(i) NO LIABILITY FOR NON-PARTICIPATION.—Nothing in this title shall be construed to subject any entity to liability for choosing not to engage in the voluntary activities authorized in this title.

(j) USE AND RETENTION OF INFORMATION.—Nothing in this title shall be construed to authorize, or to modify any existing authority of, a department or agency of the Federal Government to retain or use any information shared under this title for any use other than permitted in this title.

(k) FEDERAL PREEMPTION.—

(1) IN GENERAL.—This title supersedes any statute or other provision of law of a State or political subdivision of a State that restricts or otherwise expressly regulates an activity authorized under this title.

(2) STATE LAW ENFORCEMENT.—Nothing in this title shall be construed to supersede any statute or other provision of law of a State or political subdivision of a State concerning the use of authorized law enforcement practices and procedures.

(l) REGULATORY AUTHORITY.—Nothing in this title shall be construed—

- (1) to authorize the promulgation of any regulations not specifically authorized to be issued under this title;
- (2) to establish or limit any regulatory authority not specifically established or limited under this title; or
- (3) to authorize regulatory actions that would duplicate or conflict with regulatory requirements, mandatory standards, or related processes under another provision of Federal law.

(m) **AUTHORITY OF SECRETARY OF DEFENSE TO RESPOND TO MALICIOUS CYBER ACTIVITY CARRIED OUT BY FOREIGN POWERS.**—Nothing in this title shall be construed to limit the authority of the Secretary of Defense under section 130g of Title 10, United States Code.

(n) **CRIMINAL PROSECUTION.**—Nothing in this title shall be construed to prevent the disclosure of a cyber threat indicator or defensive measure shared under this title in a case of criminal prosecution, when an applicable provision of Federal, State, tribal, or local law requires disclosure in such case.

REPORT ON CYBERSECURITY THREATS

SEC. 109. [6 U.S.C. § 1508]

(a) **REPORT REQUIRED.**—Not later than 180 days after the date of the enactment of this Act, the Director of National Intelligence, in coordination with the heads of other appropriate elements of the intelligence community, shall submit to the Select Committee on Intelligence of the Senate and the Permanent Select Committee on Intelligence of the House of Representatives a report on cybersecurity threats, including cyber attacks, theft, and data breaches.

(b) **CONTENTS.**—The report required by subsection (a) shall include the following:

- (1) An assessment of the current intelligence sharing and cooperation relationships of the United States with other countries regarding cybersecurity threats, including cyber attacks, theft, and data breaches, directed against the United States and which threaten the United States national security interests and economy and intellectual property, specifically identifying the relative utility of such relationships, which elements of the intelligence community participate in such relationships, and whether and how such relationships could be improved.
- (2) A list and an assessment of the countries and nonstate actors that are the primary threats of carrying out a cybersecurity threat, including a cyber attack, theft, or data breach, against the United States and which threaten the United States national security, economy, and intellectual property.
- (3) A description of the extent to which the capabilities of the United States Government to respond to or prevent cybersecurity threats, including cyber attacks, theft, or data breaches, directed against the United States private sector are degraded by a delay in the prompt notification by private entities of such threats or cyber attacks, theft, and data breaches.

(4) An assessment of additional technologies or capabilities that would enhance the ability of the United States to prevent and to respond to cybersecurity threats, including cyber attacks, theft, and data breaches.

(5) An assessment of any technologies or practices utilized by the private sector that could be rapidly fielded to assist the intelligence community in preventing and responding to cybersecurity threats.

(c) **FORM OF REPORT.**—The report required by subsection (a) shall be made available in classified and unclassified forms.

(d) **INTELLIGENCE COMMUNITY DEFINED.**—In this section, the term “intelligence community” has the meaning given that term in section 3 of the National Security Act of 1947 (50 U.S.C. 3003).

EXCEPTION TO LIMITATION ON AUTHORITY OF SECRETARY OF DEFENSE TO DISSEMINATE CERTAIN INFORMATION

SEC. 110. [6 U.S.C. § 1509]

Notwithstanding subsection (c)(3) of section 393 of title 10, United States Code, the Secretary of Defense may authorize the sharing of cyber threat indicators and defensive measures pursuant to the policies, procedures, and guidelines developed or issued under this title.

EFFECTIVE PERIOD

SEC. 111. [6 U.S.C. § 1510]

(a) **IN GENERAL.**—Except as provided in subsection (b), this title and the amendments made by this title shall be effective during the period beginning on the date of the enactment of this Act and ending on September 30, 2025.

(b) **EXCEPTION.**—With respect to any action authorized by this title or information obtained pursuant to an action authorized by this title, which occurred before the date on which the provisions referred to in subsection (a) cease to have effect, the provisions of this title shall continue in effect.

TITLE II—NATIONAL CYBERSECURITY ADVANCEMENT

SUBTITLE B—FEDERAL CYBERSECURITY ENHANCEMENT

IDENTIFICATION OF INFORMATION SYSTEMS RELATING TO NATIONAL SECURITY

SEC. 228.

(a) **IN GENERAL.**—Except as provided in subsection (c), not later than 180 days after the date of enactment of this Act—

(1) the Director of National Intelligence and the Director of the Office of Management and Budget, in coordination with the heads of other agencies, shall—

(A) identify all unclassified information systems that provide access to information that may provide an adversary with the ability to derive information that would otherwise be considered classified;

(B) assess the risks that would result from the breach of each unclassified information system identified in subparagraph (A); and

(C) assess the cost and impact on the mission carried out by each agency that owns an unclassified information system identified in subparagraph (A) if the system were to be subsequently designated as a national security system; and

(2) the Director of National Intelligence and the Director of the Office of Management and Budget shall submit to the appropriate congressional committees, the Select Committee on Intelligence of the Senate, and the Permanent Select Committee on Intelligence of the House of Representatives a report that includes the findings under paragraph (1).

(b) **FORM.**—The report submitted under subsection (a)(2) shall be in unclassified form, and shall include a classified annex.

(c) **EXCEPTION.**—The requirements under subsection (a)(1) shall not apply to the Department of Defense, a national security system, or an element of the intelligence community.

(d) **RULE OF CONSTRUCTION.**—Nothing in this section shall be construed to designate an information system as a national security system.

**TITLE III—FEDERAL CYBERSECURITY WORKFORCE
ASSESSMENT**

SHORT TITLE

SEC. 301. [5 U.S.C. § 301 note]

This title may be cited as the “Federal Cybersecurity Workforce Assessment Act of 2015”.

DEFINITIONS

SEC. 302. [5 U.S.C. § 301 note]

In this title:

- (1) **APPROPRIATE CONGRESSIONAL COMMITTEES.**—The term “appropriate congressional committees” means—
 - (A) the Committee on Armed Services of the Senate;
 - (B) the Committee on Homeland Security and Governmental Affairs of the Senate;
 - (C) the Select Committee on Intelligence of the Senate;
 - (D) the Committee on Commerce, Science, and Transportation of the Senate;
 - (E) the Committee on Armed Services of the House of Representatives;
 - (F) the Committee on Homeland Security of the House of Representatives;
 - (G) the Committee on Oversight and Government Reform of the House of Representatives; and
 - (H) the Permanent Select Committee on Intelligence of the House of Representatives.
- (2) **DIRECTOR.**—The term “Director” means the Director of the Office of Personnel Management.
- (3) **NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION.**—The term “National Initiative for Cybersecurity Education” means the initiative under the national cybersecurity awareness and education program, as authorized under section 401 of the Cybersecurity Enhancement Act of 2014 (15 U.S.C. 7451).
- (4) **WORK ROLES.**—The term “work roles” means a specialized set of tasks and functions requiring specific knowledge, skills, and abilities.

NATIONAL CYBERSECURITY WORKFORCE MEASUREMENT INITIATIVE

SEC. 303. [5 U.S.C. § 301 note]

(a) **IN GENERAL.**—The head of each Federal agency shall—

- (1) identify all positions within the agency that require the performance of cybersecurity or other cyber-related functions; and
- (2) assign the corresponding employment code under the National Initiative for Cybersecurity Education in accordance with subsection (b).

(b) **EMPLOYMENT CODES.**—

(1) **PROCEDURES.**—

(A) **CODING STRUCTURE.**—Not later than 180 days after the date of the enactment of this Act, the Director, in coordination with the National Institute of Standards and Technology, shall develop a coding structure under the National Initiative for Cybersecurity Education.

(B) **IDENTIFICATION OF CIVILIAN CYBER PERSONNEL.**—Not later than 9 months after the date of enactment of this Act, the Director, in coordination with the Secretary of Homeland Security, the Director of the National Institute of Standards and Technology, and the Director of National Intelligence, shall establish procedures to implement the National Initiative for Cybersecurity Education coding structure to identify all Federal civilian positions that require the performance of information technology, cybersecurity, or other cyber-related functions.

(C) **IDENTIFICATION OF NONCIVILIAN CYBER PERSONNEL.**—Not later than 18 months after the date of enactment of this Act, the Secretary of Defense shall establish procedures to implement the National Initiative for Cybersecurity Education’s coding structure to identify all Federal noncivilian positions that require the performance of information technology, cybersecurity, or other cyber-related functions.

(D) **BASELINE ASSESSMENT OF EXISTING CYBERSECURITY WORKFORCE.**—Not later than 3 months after the date on which the procedures are developed under subparagraphs (B) and (C), respectively, the head of each Federal agency shall submit to the appropriate congressional committees of jurisdiction a report that identifies—

- (i) the percentage of personnel with information technology, cybersecurity, or other cyber-related job functions who currently hold the appropriate industry-

recognized certifications as identified under the National Initiative for Cybersecurity Education;

(ii) the level of preparedness of other civilian and noncivilian cyber personnel without existing credentials to take certification exams; and

(iii) a strategy for mitigating any gaps identified in clause (i) or (ii) with the appropriate training and certification for existing personnel.

(E) PROCEDURES FOR ASSIGNING CODES.—Not later than 3 months after the date on which the procedures are developed under subparagraphs (B) and (C), respectively, the head of each Federal agency shall establish procedures—

(i) to identify all encumbered and vacant positions with information technology, cybersecurity, or other cyber-related functions (as defined in the National Initiative for Cybersecurity Education’s coding structure); and

(ii) to assign the appropriate employment code to each such position, using agreed standards and definitions.

(2) CODE ASSIGNMENTS.—Not later than 1 year after the date after the procedures are established under paragraph (1)(E), the head of each Federal agency shall complete assignment of the appropriate employment code to each position within the agency with information technology, cybersecurity, or other cyber-related functions.

(c) PROGRESS REPORT.—Not later than 180 days after the date of enactment of this Act, the Director shall submit a progress report on the implementation of this section to the appropriate congressional committees.

IDENTIFICATION OF CYBER-RELATED WORK ROLES OF CRITICAL NEED

SEC. 304. [5 U.S.C. § 301 note]

(a) IN GENERAL.—Beginning not later than 1 year after the date on which the employment codes are assigned to employees pursuant to section 303(b)(2), and annually thereafter through 2022, the head of each Federal agency, in consultation with the Director, the Director of the National Institute of Standards and Technology, and the Secretary of Homeland Security, shall—

(1) identify information technology, cybersecurity, or other cyber-related work roles of critical need in the agency’s workforce; and

(2) submit a report to the Director that—

(A) describes the information technology, cybersecurity, or other cyber-related roles identified under paragraph (1); and

(B) substantiates the critical need designations.

(b) GUIDANCE.—The Director shall provide Federal agencies with timely guidance for identifying information technology, cybersecurity, or other cyber-related roles of critical need, including—

- (1) current information technology, cybersecurity, and other cyber-related roles with acute skill shortages; and
- (2) information technology, cybersecurity, or other cyber-related roles with emerging skill shortages.

(c) CYBERSECURITY NEEDS REPORT.—Not later than 2 years after the date of the enactment of this Act, the Director, in consultation with the Secretary of Homeland Security, shall—

- (1) identify critical needs for information technology, cybersecurity, or other cyber-related workforce across all Federal agencies; and
- (2) submit a progress report on the implementation of this section to the appropriate congressional committees.

GOVERNMENT ACCOUNTABILITY OFFICE STATUS REPORTS

SEC. 305. [5 U.S.C. § 301 note]

The Comptroller General of the United States shall—

- (1) analyze and monitor the implementation of sections 303 and 304; and
- (2) not later than 3 years after the date of the enactment of this Act, submit a report to the appropriate congressional committees that describes the status of such implementation.

TITLE IV—OTHER CYBER MATTERS

FEDERAL COMPUTER SECURITY

SEC. 406.

(a) DEFINITIONS.—In this section:

(1) COVERED SYSTEM.—The term “covered system” shall mean a national security system as defined in section 11103 of title 40, United States Code, or a Federal computer system that provides access to personally identifiable information.

(2) COVERED AGENCY.—The term “covered agency” means an agency that operates a covered system.

(3) LOGICAL ACCESS CONTROL.—The term “logical access control” means a process of granting or denying specific requests to obtain and use information and related information processing services.

(4) **MULTI-FACTOR AUTHENTICATION.**—The term “multi-factor authentication” means the use of not fewer than 2 authentication factors, such as the following:

- (A) Something that is known to the user, such as a password or personal identification number.
- (B) An access device that is provided to the user, such as a cryptographic identification device or token.
- (C) A unique biometric characteristic of the user.

(5) **PRIVILEGED USER.**—The term “privileged user” means a user who has access to system control, monitoring, or administrative functions.

(b) **INSPECTOR GENERAL REPORTS ON COVERED SYSTEMS.**—

(1) **IN GENERAL.**—Not later than 240 days after the date of enactment of this Act, the Inspector General of each covered agency shall submit to the appropriate committees of jurisdiction in the Senate and the House of Representatives a report, which shall include information collected from the covered agency for the contents described in paragraph (2) regarding the Federal computer systems of the covered agency.

(2) **CONTENTS.**—The report submitted by each Inspector General of a covered agency under paragraph (1) shall include, with respect to the covered agency, the following:

- (A) A description of the logical access policies and practices used by the covered agency to access a covered system, including whether appropriate standards were followed.
- (B) A description and list of the logical access controls and multi-factor authentication used by the covered agency to govern access to covered systems by privileged users.
- (C) If the covered agency does not use logical access controls or multi-factor authentication to access a covered system, a description of the reasons for not using such logical access controls or multi-factor authentication.
- (D) A description of the following information security management practices used by the covered agency regarding covered systems:
 - (i) The policies and procedures followed to conduct inventories of the software present on the covered systems of the covered agency and the licenses associated with such software.
 - (ii) What capabilities the covered agency utilizes to monitor and detect exfiltration and other threats, including—

- (I) data loss prevention capabilities;

(II) forensics and visibility capabilities; or

(III) digital rights management capabilities.

(iii) A description of how the covered agency is using the capabilities described in clause (ii).

(iv) If the covered agency is not utilizing capabilities described in clause (ii), a description of the reasons for not utilizing such capabilities.

(E) A description of the policies and procedures of the covered agency with respect to ensuring that entities, including contractors, that provide services to the covered agency are implementing the information security management practices described in subparagraph (D).

(3) **EXISTING REVIEW.**—The reports required under this subsection may be based in whole or in part on an audit, evaluation, or report relating to programs or practices of the covered agency, and may be submitted as part of another report, including the report required under section 3555 of title 44, United States Code.

(4) **CLASSIFIED INFORMATION.**—Reports submitted under this subsection shall be in unclassified form, but may include a classified annex.

AI ETHICS FRAMEWORK FOR THE INTELLIGENCE COMMUNITY

Artificial Intelligence (AI) can enhance the intelligence mission, but like other new tools, we must understand how to use this rapidly evolving technology in a way that aligns with our principles to prevent unethical outcomes. This is an ethics guide for United States Intelligence Community personnel on how to procure, design, build, use, protect, consume, and manage AI and related data. Answering these questions, in conjunction with your agency-specific procedures and practices, promotes ethical design of AI consistent with the Principles of AI Ethics for the Intelligence Community. This guide is not a checklist and some of the concepts discussed herein may not apply in all instances. Instead, this guide is a living document intended to provide stakeholders with a reasoned approach to judgment and to assist with the documentation of considerations associated with the AI lifecycle. In doing so, this guide will enable mission through an enhanced understanding of goals between AI practitioners and managers while promoting the ethical use of AI.

The use of AI must match the Intelligence Community's unique mission purposes, authorities, and responsibilities for collecting and using data and AI outputs. AI should:

- Be used when it is an appropriate means to achieve a defined purpose after evaluating the potential risks;
- Be used in a manner consistent with respect for individual rights and liberties of affected individuals, and use data obtained lawfully and consistent with legal obligations and policy requirements;
- Incorporate human judgment and accountability at appropriate stages to address risks across the lifecycle of the AI and inform decisions appropriately;
- Identify, account for, and mitigate potential undesired bias, to the greatest extent practicable without undermining its efficacy and utility;
- Be tested at a level commensurate with foreseeable risks associated with the use of the AI;
- Maintain accountability for iterations, versions, and changes made to the model;
- Document and communicate the purpose, limitation(s), and design outcomes;
- Use explainable and understandable methods, to the extent practicable, so that users, overseers, and the public, as appropriate, understand how and why the AI generated its outputs;
- Be periodically reviewed to ensure the AI continues to further its purpose and identify issues for resolution; and,

- Identify who will be accountable for the AI and its effects at each stage and across its lifecycle, including responsibility for maintaining records created.

Identifying and addressing risk is best achieved by involving appropriate stakeholders. As such, consumers, technologists, developers, mission personnel, risk management professionals, civil liberties and privacy officers, and legal counsel should utilize this framework collaboratively, each leveraging their respective experiences, perspectives, and professional skills. Agencies should also ensure that individuals involved in the design, development, review, deployment, and use of any AI have sufficient training to address the questions below and the issues presented above.

PURPOSE: UNDERSTANDING GOALS AND RISKS. Determine what goals you are trying to achieve to ensure you can design AI that balances desired results with acceptable risk.

- What is the goal you are trying to achieve by creating this AI, including components used in AI development? Is there a need to use AI to achieve this goal? Can you use other non-AI related methods to achieve this goal with lower risk? Is AI likely to be effective in achieving this goal?
- Are there specific AI system methods suitable and preferred for this use case? Does the efficiency and reliability of the AI in this particular use case justify its use for this purpose?
- What benefits and risks, including risks to civil liberties and privacy, might exist when this AI is in use? Who will benefit? Who or what will be at risk? What is the scale of each and likelihood of the risks? How can those risks be minimized and the remaining risks adequately mitigated? Do the likely negative impacts outweigh likely positive impacts?
- What performance metrics best suit the AI, such as accuracy, precision, and recall, based on risks determined by mission managers, analysts, and consumers given the potential risks; and how will the accuracy of the information be provided to each of those stakeholders? What impacts could false positive and false negative rates have on system performance, mission goals, and affected targets of the analysis?
- Have you engaged with the AI system developers, users, consumers, and other key stakeholders to ensure a common understanding of the goal of the AI and related risks of utilizing AI to achieve this goal?
- How are you documenting the goals and risks?

LEGAL OBLIGATIONS AND POLICY CONSIDERATIONS GOVERNING THE AI AND THE DATA. Partnering closely with risk management teams in your agency, including your legal, compliance, records management, classification, and civil liberties and privacy professionals, will help you understand governing authorities, legal obligations, information management responsibilities, and risks associated with an AI project.

- What authorities, agreements, or contracts govern the collection or acquisition of all sources of the data related to the model (training, testing, and operational data)? Who can clarify limitations from the agreements or contracts?
- What legal or policy restrictions exist on the use of data under this authority/agreement/ contract? (For example, data subject to the Privacy Act should be used for a purpose that is compatible with that for which the data was collected).
- How must data be stored, shared, retrieved, accessed, used, retained, disseminated, and dispositioned under the authority/agreement/contract, as well as relevant constitutional, statutory, and regulatory provisions?
- What authorities or agreements apply to the AI itself, including the use, modification, storage, retrieval, access, retention, and disposition of the AI? Are there any proposed downstream applications of the AI that are legally restricted from using the underlying data?
- Does combining data with other inputs from the AI create new legal, records management, or classification risks relating to how the information is maintained and protected?

HUMAN JUDGMENT AND ACCOUNTABILITY. In the Intelligence Community, the potential purposes and applications of an AI could range from basic business tasks to highly sensitive intelligence analysis. The assessed risk will determine at which point in the process and to what degree a human will be involved in the AI.

- Given the purpose of the AI and potential consequences of its use, at what points, if any, are a human required as part of the decision process? If the AI could result in significant consequences such as an action with the potential to deprive individuals of constitutional rights or the potential to interfere with their free exercise of civil liberties, how will you ensure individual human involvement and accountability in decisions that are assisted through the use of AI?
- Where and when should the human be engaged? Before the results are used in analysis? Before the outputs are provided for follow-on uses?

- Who should be the accountable human(s)? Do they know that they are designated as the accountable human(s)? What qualifications are required to serve in that role? How is accountability transferred to another human?
- What are the access controls and training requirements for those operating at different stages in the AI lifecycle?
- What does the accountable human need to know about the AI to judge its reliability and accuracy?
- How may introducing an accountable human produce cognitive biases and/or confirmation bias?
- Who should be engaged for unresolved issues and disputes regarding the AI or its outputs?

MITIGATING UNDESIREB BIAS AND ENSURING OBJECTIVITY. Ensuring objectivity is a defining characteristic of intelligence analysis. In conducting analysis, Intelligence Community Directive 203 requires that we must perform our functions “with objectivity and with awareness of [our] own assumptions and risks. [We] must employ reasoning techniques and practical mechanisms that reveal and mitigate bias.” For legal, policy, and mission reasons, however, there are certain “biases” that the Intelligence Community intentionally introduces as it designs, develops, and uses AI. Specifically, we design our models and choose our datasets to screen out irrelevant information, focus on the specific foreign intelligence targets, and appropriately minimize the collection and use of United States person information. In mitigating bias, the Intelligence Community therefore focuses on identifying and minimizing undesired bias. “Undesired bias” is bias that could undermine analytic validity and reliability, harm individuals, or impact civil liberties such as freedom from undue government intrusion on speech, religion, travel, or privacy. Undesired bias may be introduced through the process of data collection, feature extraction, curating/labeling data, model selection and development, and even in user training. Taking steps to discover bias throughout the lifecycle of an AI, mitigate undesired bias, and to document and communicate known biases and how they were addressed, are critical to long-term reliance on training data sets, to reusing models, and to trusting outputs for follow-on use.

- How complete are the data on which the AI will rely? Are they representative of the intended domain? How relevant is the training and evaluation data to the operational data and context? How does the AI avoid perpetuating historical biases and discrimination?

- What are the correct metrics to assess the AI's output? Is the margin of error one that would be deemed tolerable by those who use the AI? What is the impact of using inaccurate outputs and how well are these errors communicated to the users?
- What are the potential tradeoffs between reducing undesired bias and accuracy? To what extent can potential undesired bias be mitigated while maintaining sufficient accuracy?
- Do you know or can you learn what types of bias exist in the training data (statistical, contextual, historical, or other)? How can undesired bias be mitigated? What would happen if it is not mitigated? Is the selected testing data appropriately representative of the training data? Based on the purpose of the AI, how much and what kind of bias, if any, are you willing to accept in the data, model, and output? Is the team diverse enough in disciplinary, professional, and other perspectives to minimize any human bias?
- How will undesired bias and potential impacts of the bias, if any, be communicated to anyone who interacts with the AI and output data?

TESTING YOUR AI. Every system must be tested for accuracy in an environment that controls for known and reasonably foreseeable risks prior to being deployed.

- Based on the purpose of the AI and potential risks, what level of objective performance for the desired performance metric, (e.g., precision, recall, accuracy, etc.) do you require?
- Has the AI been evaluated for potential biased outcomes or if outcomes cause an inappropriate feedback loop? Have you considered applicable methods to make the AI more robust to adversarial attacks?
- How and where will you document the test methodology, results, and changes made based on the test results?
- If a third party created the AI, what additional risks may be associated with that third party's assumptions, motives, and methodologies? What limitations might arise from that third party claiming its methodology is proprietary? What information should you require as part of the acquisition of the analytic? What is the minimum amount of information you must have to approve an AI for use?
- Was the AI tested for potential security threats in any/all levels of its stack (e.g. software level, AI framework level, model level, etc.)? Were resulting risks mitigated?

ACCOUNTING FOR BUILDS, VERSIONS, AND EVOLUTIONS OF AN AI. A successful AI is often refined through numerous iterations, versions, or evolutions, both while it is being trained on training data and after it matures and is applied to

mission, analytic, and business data. An existing AI may also be repurposed and require modifications and/or retraining prior to redeployment.

- As you refine the AI, how does the data you have used, the parameters and weights you have chosen, and the outputs ensure that this version or evolution is designed to achieve the authorized purpose?
- Have you accounted for natural data drift within the operational environment compared to training data?
- Have you documented provenance of data, outputs of the iteration, and test results (accuracy) in a way that will provide for repeatability, auditing, and oversight? If the AI is continuously modified, are all critical aspects, dependencies, and artifacts version controlled and documented? Will it be clear to anyone auditing the AI or consumers of the AI's outputs which version was in use at any given moment in time? Will it be clear which iteration of a model drew on which data and produced what outputs?
- Where will you save documentation on versions of AI and relevant training and test data? Have you made that information available to users and consumers of the AI? How will this documentation be retained and made discoverable to ensure compliance with your Agency's records management responsibilities?
- Have you accounted for changes in demographics of your customer for your AI capability (e.g., changing user experience needs) or the changing needs of the mission?

DOCUMENTATION OF PURPOSE, PARAMETERS, LIMITATIONS, AND DESIGN OUTCOMES. To ensure your AI is used properly, it is important to communicate (a) what the AI is for, (b) what it is not for, (c) how it was designed, and (d) what its limitations are. Documentation assists not only with proper management of the AI, but also with determining whether the AI is appropriate for new purposes that were not originally envisioned.

- How can you store the documentation in a way that is available to all potential consumers of this AI?
- Have you documented where the data came from and its downstream uses and sharability? The downstream uses and sharability of the AI?
- Have you documented what rules apply to the data as a whole? What rules apply to subsets?
- Have you documented the potential risks of using the AI and its output data, and the steps taken to minimize these risks?
- Have you documented use cases for which the AI was and was not specifically designed?
- Have you documented the process for discovering undesired bias and the conclusions?

- Have you documented how to verify and validate the model as well as the frequency with which these checks should be performed?

TRANSPARENCY: EXPLAINABILITY AND INTERPRETABILITY. AI can achieve the anticipated outcome despite using inappropriate criteria. Consistent with the Principles of Intelligence Transparency for the Intelligence Community, use methods that are explainable and understandable, to the extent practicable, so that users, overseers, and the public, as appropriate, understand how and why the AI generated its outputs.

- Given the purpose of the AI, what level of explainability or interpretability is required for how the AI made its determination? If a third party created the AI, how will you ensure a level of explainability or interpretability? Does this conform with Intelligence Community Directive 203: Analytic Standards?
- How are outputs marked to clearly show that they came from an AI?
- How might you respond to an intelligence consumer asking “How do you know this?” How will you describe the dataset(s) and tools used to make the output? How was the accuracy or appropriate performance metrics assessed? How were the results independently verified? Have you documented and explained that machine errors may differ from human errors?

PERIODIC REVIEW. All AI should be checked at an appropriate documented interval to determine whether it still meets its purpose and that any undesired biases or unintended outcomes are appropriately mitigated.

- How will user and peer engagement be integrated into the model development process and periodic performance review once deployed?
- Given the purpose of this AI, what is an appropriate interval for checking whether it is still accurate, unbiased, explainable, etc.? What are the checks for this model?
- As time passes and conditions change, is the training data still representative of the operational environment?
- How will the appropriate performance metrics, such as accuracy, of the AI be monitored after the AI is deployed? How much distributional shift or model drift from baseline performance is acceptable?
- Who is responsible for checking the AI at these intervals?
- How will the accountable human(s) address changes in accuracy and precision due to either an adversary’s attempts to disrupt the AI or unrelated changes in the operational/business environment, which may impact the accuracy of the AI?

STEWARDSHIP AND ACCOUNTABILITY: TRAINING DATA, ALGORITHMS, MODELS, OUTPUTS OF THE MODELS, DOCUMENTATION. Before the AI is deployed, it must

be clear who will have the responsibility for the continued maintenance, monitoring, updating, and decommissioning of the AI.

- Who will be responsible for maintaining, re-verifying, monitoring, and updating this AI once deployed?
- Who is ultimately responsible for the decisions of the AI and is this person aware of the intended uses and limitations of the analytic?
- Who is accountable for the ethical considerations during all stages of the AI lifecycle?
- If anyone believed that the AI no longer meets this ethical framework, who will be responsible for receiving the concern and as appropriate investigating and remediating the issue? Do they have authority to modify, limit, or stop the use of the AI?

**INTELLIGENCE SHARING PROCEDURES FOR FOREIGN
INTELLIGENCE AND FOREIGN COUNTERINTELLIGENCE
INVESTIGATIONS CONDUCTED BY THE
FEDERAL BUREAU OF INVESTIGATION**

OFFICE OF THE ATTORNEY GENERAL
WASHINGTON, D.C. 20530

March 6, 2002

MEMORANDUM

TO: Director, FBI
Assistant Attorney General, Criminal Division
Counsel for Intelligence Policy
United States Attorneys

FROM: The Attorney General -/S/-John Ashcroft

SUBJECT: Intelligence Sharing Procedures for Foreign Intelligence and Foreign
Counterintelligence Investigations Conducted by the FBI

I. INTRODUCTION AND STATEMENT OF GENERAL PRINCIPLES

Unless otherwise specified by the Attorney General, these procedures apply to foreign intelligence (FI) and foreign counterintelligence (FCI) investigations conducted by the Federal Bureau of Investigations (FBI). They are designed to ensure that FI and FCI investigations are conducted lawfully, particularly in light of requirements imposed by the Foreign Intelligence Surveillance Act (FISA), and to promote the effective coordination and performance of the criminal and counterintelligence functions of the Department of Justice (DOJ). These procedures supersede the procedures adopted by the Attorney General on July 19, 1995 (including the annex concerning the Southern District of New York), the interim measures approved by the Attorney General on January 21, 2000, and the memorandum issued by the Deputy Attorney General on August 6, 2001. Terms used in these procedures shall be interpreted in keeping with definitions contained in FISA. References in these procedures to particular positions or

INTELLIGENCE SHARING PROCEDURES FOR FOREIGN INTELLIGENCE AND
FOREIGN COUNTERINTELLIGENCE INVESTIGATIONS CONDUCTED BY THE FBI

components within the Department of Justice shall apply to any successor position or component.

Prior to the USA Patriot Act, FISA could be used only for the “primary purpose” of obtaining “foreign intelligence information.” The term “foreign intelligence information” was and is defined to include information that is necessary, or relevant, to the ability of the United States to protect against foreign threats to national security, such as attack, sabotage, terrorism, or clandestine intelligence activities. See 50 U.S.C. § 1801(e)(1). Under the primary purpose standard, the government could have a significant law enforcement purpose for using FISA, but only if it was subordinate to the primary foreign intelligence purpose. The USA PATRIOT Act allows FISA to be used for “a significant purpose,” rather than the primary purpose, of obtaining foreign intelligence information. Thus, it allows FISA to be used primarily for a law enforcement purpose, as long as a significant foreign intelligence purpose remains. See U.S.C. § 1804(a)(7)(B), 1823(a)(7)(B).

The Act also expressly authorizes intelligence officers who are using FISA to “consult” with federal law enforcement officers to “coordinate efforts to investigate or protect against” foreign threats to national security. Under this authority, intelligence and law enforcement officers may exchange a full range of information and advice concerning such efforts in FI or FCI investigations, including information and advice designed to preserve or enhance the possibility of a criminal prosecution. The USA Patriot Act provides that such consultation between intelligence and law enforcement officers “shall not” preclude the government’s certification of a significant foreign intelligence purpose or the issuance of a FISA warrant. See 50 U.S.C. §§ 1806(k), 1825(k).

Consistent with the USA Patriot Act and with standards of effective management, all relevant DOJ components, including the Criminal Division, the relevant United States Attorney’s Offices (USAOs), and the Office of Intelligence Policy and Review (OIPR), must be fully informed about the nature, scope, and conduct of all full field FI and FCI investigations, whether or not those investigations involve the use of FISA. Correspondingly, the Attorney General can most effectively direct and control such FI and FCI investigation only if all relevant DOJ components are free to offer advice and make recommendations, both strategic and tactical, about the conduct and goals of the investigations. The overriding need to protect the national security from foreign threats compels a full and free exchange of information and ideas.

II. INTELLIGENCE SHARING PROCEDURES CONCERNING THE CRIMINAL DIVISION

(A) DISSEMINATING INFORMATION.

The Criminal Division and OIPR shall have access to all information developed in full field FI and FCI investigations except as limited by orders issued by the Foreign Intelligence Surveillance Court, controls imposed by the originator of sensitive material, and restrictions established by the Attorney General or the Deputy Attorney General in particular cases. See 50 U.S.C §§1801 (h), 1806 (a), 1825 (a).

The FBI shall keep the Criminal Division and OIPR apprised of all information developed in full field FI and FCI investigations that is necessary to the ability of the United States to investigate or protect against foreign attack, sabotage, terrorism, and clandestine intelligence activities, subject to the limits set forth above. Relevant information includes both foreign intelligence information and information concerning a crime which has been, is being, or is about to be committed. The Criminal Division and OIPR must have access to this information to ensure the ability of the United States to coordinate efforts to investigate and protect against foreign threats to national security, including protection against such threats through criminal investigation and prosecution, and in keeping with the need of the United States to obtain, produce, and disseminate foreign intelligence information. See 50 U.S.C. §§ 1801(h)(1), 1806(k), 1825(k).

The FBI shall also keep the Criminal Division and OIPR apprised of information developed in full field FI and FCI investigations that concerns any crime which has been, is being, or is about to be committed. See U.S.C § 1801(h)(3).

As part of its responsibility under the preceding paragraphs, the FBI shall provide to the Criminal Division and OIPR copies of annual Letterhead Memoranda (or successor summary documents) in all full field FI and FCI investigation, and shall make available to the Criminal Division and OIPR relevant information from investigative files, as appropriate. The Criminal Division shall adhere to any reasonable conditions on the storage and disclosure of such documents and information that the FBI or OIPR may require.

INTELLIGENCE SHARING PROCEDURES FOR FOREIGN INTELLIGENCE AND
FOREIGN COUNTERINTELLIGENCE INVESTIGATIONS CONDUCTED BY THE FBI

All information acquired pursuant to a FISA electronic surveillance or physical search that is disseminated to the Criminal Division shall be accompanied by a statement that such information, or any information derived therefrom, may only be used in any criminal proceeding (including search and arrest warrant affidavits and grand jury subpoenas and proceedings) with the advance authorization of the Attorney General. See 50 U.S.C. §§ 1806(b), 1825(c).

(B) PROVIDING ADVICE.

The FBI, the Criminal Division, and OIPR shall consult with one another concerning full field FI and FCI investigations except as limited by these procedures, orders issued by the Foreign Intelligence Surveillance Court, and restrictions established by the Attorney General or the Deputy Attorney General in particular cases.

Consultations may include the exchange of advice and recommendations on all issues necessary to the ability of the United States to investigate or protect against foreign attack, sabotage, terrorism, and clandestine intelligence activities, including protection against the foregoing through criminal investigations and prosecution, subject to the limits set forth above. Relevant issues include, but are not limited to, the strategy and goals for the investigation; the law enforcement and intelligence methods to be used in conducting the investigation; the interaction between intelligence and law enforcement components as part of the investigation; and the initiation, operation, continuation, or expansion of FISA searches or surveillance. Such consultations are necessary to the ability of the United States to coordinate efforts to investigate and protect against foreign threats to national security as set forth in 50 U.S.C. §§ 1806(k), 1825(k).

The FBI, the Criminal Division, and OIPR shall meet regularly to conduct consultations. Consultations may also be conducted directly between two or more components at any time. Disagreements arising from consultations may be presented to the Deputy Attorney General or the Attorney General for resolution.

III. INTELLIGENCE SHARING PROCEDURES CONCERNING A USAO

With respect to FI or FCI investigation involving international terrorism, the relevant USAOs shall receive information and engage in consultations to the same extent as the Criminal Division under Parts II.A and II.B of these

INTELLIGENCE SHARING PROCEDURES FOR FOREIGN INTELLIGENCE AND
FOREIGN COUNTERINTELLIGENCE INVESTIGATIONS CONDUCTED BY THE FBI

procedures. Thus, the relevant USAOs shall have access to information developed in full field investigations, shall be kept apprised of information necessary to protect national security, shall be kept apprised of information concerning crimes, shall receive copies of LHMs or successor summary documents, and shall have access to the FBI files to the same extent as the Criminal Division. The relevant USAOs shall receive such information and access from the FBI field offices. The relevant USAOs also may and shall engage in regular consultations with the FBI and OIPR to the same extent as the Criminal Division.

With respect to FI or FCI investigations involving espionage, the Criminal Division shall, as appropriate, authorize the dissemination of information to a USAO, and shall also, as appropriate, authorize consultations between the FBI and a USAO, subject to the limits set forth in Parts II.A and II.B of these procedures. In an emergency, the FBI may disseminate information to, and consult with, a United States Attorney's Office concerning an espionage investigation without the approval of the Criminal Division, but shall notify the Criminal Division as soon as possible after the fact.

All information disseminated to a USAO pursuant to these procedures, whether or not the information is derived from FISA and whether or not it concerns a terrorism or espionage investigation, shall be disseminated only to the United States Attorney (USA) and/or any Assistant United States Attorneys (AUSUAs) designated to the Department of Justice by the USA as points of contact to receive such information. The USAs and the designated AUSAs shall have appropriate security clearances and shall receive training in the handling of classified information and information derived from FISA, including training concerning restrictions on the use and dissemination of such information.

Except in an emergency, where circumstances preclude the opportunity of consultation, the USAOs shall take no action on the information disseminated pursuant to these procedures without consulting with the Criminal Division and OIPR. The term "action" is defined to include the use of such information in any criminal proceeding (including search and arrest warrant affidavits and grand jury subpoenas and proceedings), and the disclosure of such information to a court or to any non-government personnel. See also U.S. Attorney's Manual §§9-2.136, 9-90.020. Disagreements arising from consultations pursuant to this paragraph may be presented to the Deputy Attorney General or the Attorney General for resolution.

INTELLIGENCE SHARING PROCEDURES FOR FOREIGN INTELLIGENCE AND
FOREIGN COUNTERINTELLIGENCE INVESTIGATIONS CONDUCTED BY THE FBI

All information acquired pursuant to a FISA electronic surveillance or physical search that is disseminated to a USAO shall be accompanied by a statement that such information, or any information derived therefrom, may only be used in any criminal proceeding (including search and arrest warrant affidavits and grand jury subpoenas and proceedings) with the advance authorization of the Attorney General. See 50 U.S.C. §§ 1806(b), 1835(c). Whenever a USAO requests authority from Attorney General to use such information in a criminal proceeding, it shall simultaneously notify the Criminal Division.

**DISCLOSURE OF FOREIGN INTELLIGENCE ACQUIRED IN THE COURSE OF A
CRIMINAL INVESTIGATION GUIDELINES**

**GUIDELINES REGARDING DISCLOSURE TO THE DIRECTOR OF
CENTRAL INTELLIGENCE AND HOMELAND SECURITY OFFICIALS
OF FOREIGN INTELLIGENCE ACQUIRED IN THE COURSE OF A
CRIMINAL INVESTIGATION**

OFFICE OF THE ATTORNEY GENERAL
WASHINGTON, DC 20530

September 23, 2002

MEMORANDUM FOR HEADS OF DEPARTMENT OF JUSTICE
COMPONENTS AND HEADS OF FEDERAL DEPARTMENTS
AND AGENCIES WITH LAW ENFORCEMENT
RESPONSIBILITIES

FROM: The Attorney General -/S/-John Ashcroft

SUBJECT: Guidelines Regarding Disclosure to the Director of Central
Intelligence and Homeland Security Officials of Foreign
Intelligence Acquired in the course of a Criminal Investigation

BACKGROUND

The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. 107-56, 115 Stat. 272, 389, enacted into law certain requirements for the sharing of information by Federal law enforcement agencies with the intelligence community. Specifically, section 905(a) of the USA PATRIOT Act provides that “the Attorney General, or the head of any other department or agency of the Federal Government with law enforcement responsibilities, shall expeditiously disclose to the Director of Central Intelligence, pursuant to guidelines developed by the Attorney General in consultation with the Director, foreign intelligence acquired by an element of the Department of Justice or an element of such department or agency, as the case may be, in the course of a criminal investigation.”

Since the enactment of the USA PATRIOT Act, federal law enforcement agencies have taken steps to improve existing channels of communication with the intelligence community and certain offices relating to homeland security (collectively, “Receiving Agencies”) in order to share foreign intelligence

DISCLOSURE OF FOREIGN INTELLIGENCE ACQUIRED IN THE COURSE OF A CRIMINAL INVESTIGATION GUIDELINES

acquired in the course of criminal investigations. The purpose of these guidelines is to formalize a framework pursuant to section 905(a) of the USA PATRIOT Act that will facilitate and increase to the fullest extent possible the continued expeditious sharing of such information. The procedures established by these guidelines for the sharing of information between components of the Department of Justice or other departments and agencies having law enforcement responsibilities with Recipients (as defined below) are not, however, intended to replace or supersede existing operational or information sharing mechanisms between Federal law enforcement agencies and Receiving Agencies. As appropriate, those relationships should continue to be used to the fullest extent possible.

Heads of Department of Justice components and heads of other departments and agencies of the Federal government having law enforcement responsibility shall distribute these guidelines within their respective departments, components and agencies, as appropriate, to ensure prompt and effective implementation of section 905(a) and these guidelines.

GUIDELINES FOR SECTION 905(A) INFORMATION SHARING

(1) SCOPE OF APPLICATION. These guidelines apply to all elements of the Department of Justice having criminal investigative or prosecutorial responsibilities and to all other departments and agencies of the Federal government having law enforcement responsibilities (hereinafter, collectively, “Federal Law Enforcement Agencies”). These guidelines do not apply to agencies that provide support to criminal investigations, but that do not themselves conduct criminal investigations (e.g., the Department of Treasury’s Office of Foreign Assets Control and Financial Crimes Enforcement Network).

(2) LAW ENFORCEMENT INFORMATION SUBJECT TO MANDATORY DISCLOSURE. Subject to any exceptions established by the Attorney General in consultation with the Director of Central Intelligence (the “Director”) and Assistant to the President for Homeland Security, section 905(a) and these guidelines require expeditious disclosure to the Director, the Assistant to the President for Homeland Security or other members of the U.S. intelligence community or homeland security agencies as are designated under paragraph 4, *infra*, of foreign intelligence acquired in the course of a criminal investigation conducted by Federal Law Enforcement Agencies.

(a) As used herein, the term “foreign intelligence” is defined in section 3 of the National Security Act of 1947 (50 U.S.C. § 401a) as: “information relating to the capabilities, intentions, or activities of foreign

DISCLOSURE OF FOREIGN INTELLIGENCE ACQUIRED IN THE COURSE OF A CRIMINAL INVESTIGATION GUIDELINES

governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities.”

(b) The term “section 905(a) information” means foreign intelligence acquired in the course of a criminal investigation.

(c) Section 203(d) of the USA PATRIOT Act, provides that:

“Notwithstanding any other law, it shall be lawful for foreign intelligence or counterintelligence (as defined in section 3 of the National Security Act of 1947 (50 U.S.C §401a)) or foreign intelligence information obtained as part of a criminal investigation to be disclosed to any Federal law enforcement, intelligence, protective, immigration, national defense, or national security official in order to assist the official receiving that information in the performance of his official duties.”

Thus, no other Federal or state law operates to prevent the sharing of such information so long as disclosure of such information will assist the Director and the Assistant to the President for Homeland Security in the performance of their official duties, and Federal Law Enforcement Agencies shall, notwithstanding any other law, expeditiously disclose to the Recipients (as defined below) section 905(a) information.

(3) TRAINING. Pursuant to section 908 of the USA PATRIOT Act, the Department of Justice, in consultation with the Director, the Assistant to the President for Homeland Security, and other Federal Law Enforcement Agencies, will develop a training curriculum and program to ensure that law enforcement officials receive sufficient training to identify foreign intelligence subject to the disclosure requirements under these guidelines.

(4) ENTITIES TO WHOM DISCLOSURE SHALL BE MADE. The Director, in consultation with the Assistant to the President for Homeland Security, shall promptly advise the Attorney General of his designations of appropriate offices, entities and/or officials of Receiving Agencies to receive the disclosure of section 905(a) information not covered by an established operational or information sharing mechanism. Said designees, together with the Director and the Assistant to the President for Homeland Security and all offices, entities, or individuals covered by such an established mechanism, are collectively referred to herein as the “Recipients.” The Director, in consultation with the Assistant to the President for Homeland Security, shall ensure that sufficient Recipients are identified to facilitate expeditious sharing and handling of section 905(a) information.

(5) METHODS FOR DISCLOSURE OF SECTION 905(A) INFORMATION. Subject only to any exceptions that may be established pursuant to paragraph 9(a), *infra*, all section 905(a) information shall be shared as expeditiously as possible with one or more of the Recipients. The procedures established in this paragraph may be supplemented by more detailed definitions and protocols disseminated to

DISCLOSURE OF FOREIGN INTELLIGENCE ACQUIRED IN THE COURSE OF A CRIMINAL INVESTIGATION GUIDELINES

appropriate law enforcement, intelligence, and homeland security officials in classified or confidential form.

(a) **TERRORISM OR WEAPONS OF MASS DESTRUCTION (WMD) INFORMATION.** Federal law enforcement officials shall disclose immediately to one or more Recipients information which they reasonably believe relates to a potential terrorism or WMD threat to the United States homeland, its critical infrastructure, key resources (whether physical or electronic), or to United States persons or interests worldwide. Other terrorism or WMD information, as defined by section 5(a)(i) and (ii), shall be disclosed to one or more Recipients as expeditiously as possible. In all cases, the official shall disclose such information with the understood priorities of disrupting terrorist plans, preventing terrorists' attacks, and preserving the lives of United States persons. Disclosure may be made through one or more of the following: existing field-level operational or information sharing mechanisms, including a Joint Terrorism Task Force (JTTF); existing headquarters operational or information sharing mechanisms; or when the officer reasonably believes that time does not permit the use of any such established mechanisms, any other field level or other mechanism intended to facilitate immediate action, response or other efforts to address such threats.

As soon as possible after any disclosure under the preceding paragraph, the disclosing official shall notify the relevant JTTF of the disclosure. The JTTF shall, as appropriate, keep the relevant Anti-Terrorism Task Force (ATTF) apprised of the nature of the information disclosed. The relevant ATTF shall, in turn, apprise the Department of Justice Criminal Division's Terrorism and Violent Crime Section (TVCS). Where information is disclosed by the headquarters of the relevant Federal Law Enforcement Agency, the headquarters shall, as soon as practicable and to the extent reasonable, notify TVCS of all disclosures. Federal agencies may require additional notification procedures where appropriate.

For purposes of these guidelines, "terrorism information" and "weapons of mass destruction information" are defined as follows:

TERRORISM INFORMATION: All information relating to the existence, organization, capabilities, plans, intentions, vulnerabilities, means of finance or material support, or activities of foreign or international terrorist groups or individuals or threats posed by such groups or individuals to the United States, United

DISCLOSURE OF FOREIGN INTELLIGENCE ACQUIRED IN THE COURSE OF A CRIMINAL INVESTIGATION GUIDELINES

States persons, or United States interests, or to those of other nations, or to communications between such groups or individuals, or information relating to groups or individuals reasonably believed to be assisting or associated with them.

WEAPONS OF MASS DESTRUCTION (WMD) INFORMATION: All information relating to conventional explosive weapons and non-conventional weapons capable of causing mass casualties and damage, including chemical, biological, radiological and nuclear agents and weapons and the means of delivery of such weapons.

(b) **ALL OTHER SECTION 905(A) INFORMATION.** In consultation with the Department of Justice and the Director, Federal Law Enforcement Agencies shall develop (or continue to follow existing) protocols (which may be classified or confidential) to provide for the expeditious sharing of section 905(a) information concerning all other subjects.

(c) **CONSULTATION WITH RESPECT TO TITLE III AND GRAND JURY MATERIALS.** Except as to section 905(a) information related to a potential terrorism or WMD threat, disclosure of 905(a) information will be accomplished in consultation with the prosecuting official assigned to the case if: (i) the information was developed through investigatory activities occurring after a particular investigation has been referred formally to the Department of Justice for prosecution; and (ii) the information was produced by an electronic, wire, or oral interception or solely as a result of a grand jury subpoena or testimony occurring before a grand jury receiving information concerning the particular investigation. This consultation may be the basis for identifying appropriate use restrictions or for seeking an exception to the section 905(a) disclosure requirements as set forth in paragraph 9, *infra*. Consultation shall be accomplished expeditiously, and any resulting disclosure shall occur no later than 48 hours after the prosecutor is initially notified. Section 905(a) information that a Federal law enforcement official reasonably believes is related to a potential terrorism or WMD threat, including information received from an electronic, wire, or oral interception or as a result of a grand jury subpoena or testimony occurring before a grand jury, shall be immediately disclosed by the Federal law enforcement official using the mechanisms described in paragraph 5(a), *supra*, and without need for advance consultation with the prosecuting official responsible for the case. Contemporaneously or as soon after making the disclosure as possible, the Federal law enforcement official shall notify the

DISCLOSURE OF FOREIGN INTELLIGENCE ACQUIRED IN THE COURSE OF A CRIMINAL INVESTIGATION GUIDELINES

prosecuting official responsible for the case in order to facilitate notice to the court, if necessary or appropriate.

(6) REQUESTS FOR ADDITIONAL INFORMATION AND AMPLIFICATION ON INITIAL DISCLOSURE.

(a) Initial disclosure of section 905(a) information to Recipients shall be accomplished automatically and without specific prior request to the disclosing department, component, or agency.

(b) Requests by any Recipient for additional information or for clarification or amplification related to the initial disclosure should be coordinated, as applicable, through the component that provided the initial information or the designated headquarters office of the relevant Federal law enforcement agency.

(7) DISCLOSURE OF GRAND JURY AND ELECTRONIC, WIRE, AND ORAL INTERCEPTION INFORMATION.

(a) Sections 203(a) and (b) of the USA PATRIOT Act permit the disclosure of federal grand jury information and electronic, wire and oral interception information to specified recipients for specified purposes (hereinafter “section 203 information”).

(b) Where section 203 information is shared pursuant to Paragraph 5, notice of such disclosures shall be promptly provided to the Office of Enforcement Operations (OEO) of the Department of Justice, Criminal Division. OEO shall establish appropriate record keeping procedures to ensure compliance with notice requirements related to the disclosure of grand jury information pursuant to section 203.

(c) The USA PATRIOT Act requires special procedures for the disclosure of section 203 information that identifies United States persons. The Federal law enforcement agency disclosing section 203 information pursuant to these guidelines shall observe the procedures established by the Attorney General for disclosing such information that identifies a United States person. A copy of the section 203 United States person information procedures is attached as Appendix B.

(d) By these guidelines the special procedures that were established pursuant to section 203(c) are made applicable to all section 905(a) disclosures of information that identify a United States person.

(8) INFORMATION USE RESTRICTIONS.

(a) In the absence of any significant law enforcement interests, as identified below in paragraph 8(b), necessitating the imposition of use restrictions, Federal Law Enforcement Agencies shall disclose section 905(a) information to Recipients pursuant to these guidelines free of any originator controls or information use restrictions.

DISCLOSURE OF FOREIGN INTELLIGENCE ACQUIRED IN THE COURSE OF A CRIMINAL INVESTIGATION GUIDELINES

(b) The originator of the section 905(a) information may impose appropriate use restrictions necessary to protect sensitive law enforcement sources and ongoing criminal investigations and prosecutions. The scope and duration of such restrictions, including caveats restricting use of the disclosed information to a particular level or element of the intelligence community, will be tailored to address the particular situation or subject matter involved.

(i) When imposed, use restrictions shall be no more restrictive than necessary to accomplish the desired effect.

(ii) Once imposed, use restrictions shall be reviewed periodically by the originator to determine whether they can be narrowed or lifted at the request of Recipients.

(c) Section 203 information shall be disclosed subject to any use restrictions necessary to comply with notice and record keeping requirements and to protect sensitive law enforcement sources and ongoing criminal investigations and prosecutions.

(9) ATTORNEY GENERAL EXCEPTIONS TO MANDATORY DISCLOSURE OF SECTION 905 INFORMATION.

(a) Section 905(a) expressly authorizes the Attorney General, in consultation with the Director, to exempt by regulation from the mandatory disclosure obligation one or more classes of foreign intelligence or foreign intelligence related to one or more targets or matters.

(b) Pending the development of appropriate permanent exceptions, exemptions from the mandatory disclosure obligation will be determined by the Attorney General in consultation with the Director and the Assistant to the President for Homeland Security on a case-by-case basis.

(c) Requests for an Attorney General exception to mandatory disclosure of section 905(a) information must be submitted by the department, component or agency head in writing with a complete description of the facts and circumstances giving rise to the need for an exception and why lesser measures such as use restrictions are not adequate.

(10) **ADMINISTERING AGENT.** The Assistant Attorney General of the Criminal Division, in consultation with affected Agencies, Offices and Divisions of the Department of Justice, will act as executive agent for the Attorney General in administering these guidelines and providing advice and assistance to Federal law enforcement regarding the implementation of sections 203 and 905.

(11) **NO PRIVATE RIGHTS CREATED.** These procedures are not intended to and do not create any rights, privileges, or benefits, substantive or procedural,

**DISCLOSURE OF FOREIGN INTELLIGENCE ACQUIRED IN THE COURSE OF A
CRIMINAL INVESTIGATION GUIDELINES**

enforceable by any party against the United States, its departments, agencies, or other entities, its officers or employees, or any other person.

(12) EFFECTIVE IMMEDIATELY. The guidelines in this memorandum shall be effective immediately.

APPENDICES:

A. Extract Copy of Section 905

B. Procedures for Marking, Handling and Disclosing Information that Identifies a United States Person

**REPORTS OF POSSIBLE CRIMINAL ACTIVITY INVOLVING FOREIGN
INTELLIGENCE SOURCES GUIDELINES**

**GUIDELINES REGARDING PROMPT HANDLING OF REPORTS
OF POSSIBLE CRIMINAL ACTIVITY INVOLVING
FOREIGN INTELLIGENCE SOURCES**

OFFICE OF THE ATTORNEY GENERAL
WASHINGTON, DC 20530

September 23, 2002

MEMORANDUM FOR HEADS OF DEPARTMENT COMPONENTS

FROM: The Attorney General -/S/-John Ashcroft

SUBJECT: Guidelines Regarding Prompt Handling of Reports of Possible
Criminal Activity Involving Foreign Intelligence Sources

Section 905(b) of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. 107-56, 115 Stat. 272,389, requires the Attorney General to develop guidelines to ensure that the Department of Justice responds within a reasonable period of time to reports from the intelligence community of possible criminal activity involving foreign intelligence sources or potential foreign intelligence sources. See [50 U.S.C. § 3040(b)]. This memorandum establishes procedures to administer the requirements of section 905(b).

Pursuant to section 1.7(a) of Executive Order 12333; 28 U.S.C. § 535(b); and the *1995 Memorandum of Understanding: Reporting of Information Concerning Federal Crimes* (“1995 MOU”) between the Department of Justice and members of the intelligence community (Attachment A hereto), the intelligence community is required, inter alia, to report to the Assistant Attorney General or a designated Deputy Assistant Attorney General of the Criminal Division information that it has collected in the performance of its intelligence activities concerning possible federal crimes by employees of an intelligence agency and violations of specified federal criminal laws by any other person. This reporting requirement extends to matters in which the intelligence community agency determines that investigation or prosecution of the matter “may result in a public disclosure of classified information or intelligence sources or methods or would jeopardize the security of ongoing intelligence operations.” 1995 MOU at 9.

REPORTS OF POSSIBLE CRIMINAL ACTIVITY INVOLVING FOREIGN INTELLIGENCE SOURCES GUIDELINES

Upon receipt of a report of possible criminal activity pursuant to the 1995 MOU, the designated Deputy Assistant Attorney General shall refer the possible crime report to the appropriate component within the Department of Justice for review, including a determination of whether to commence or decline to commence a criminal investigation.

Section 905(b) reflects a recognition that when the possible criminal activities involve a foreign intelligence source or potential foreign intelligence source, the referring intelligence community agency may have a strong interest in knowing on an expedited basis whether the Department of Justice intends to investigate potential crimes.

Accordingly, I hereby direct that, when an intelligence community agency making such a possible crime report (all of which fall within the scope of and therefore should be made pursuant to the 1995 MOU) to the Criminal Division of the Department:

- (1) notifies the Assistant Attorney General or designated Deputy Assistant Attorney General¹ that the possible crime report involves activity of a foreign intelligence source or potential foreign intelligence source; and
- (2) requests an expedited determination of the Department of Justice's intent to commence or decline to commence a criminal investigation,

the designated Deputy Assistant Attorney General and/or another attorney within the Criminal Division or other relevant component of the Department shall expeditiously confer with the referring intelligence community agency about the possible criminal activity, the reasons for the time sensitivity, and the nature and extent of the intelligence equities that may be affected by a decision to commence or decline to commence a criminal investigation of the reported activity. Upon receipt of the report, the designated Deputy Assistant Attorney General shall determine whether immediate contact with the referring agency is necessary. If a need for immediate contact is not established, an appropriate Department attorney will be made available for an initial contact with the referring intelligence community agency within seven days of the receipt of the report requesting an expedited determination.

¹ The notification should be documented in writing, consistent with the procedures set forth in the 1995 Memorandum of Understanding governing the reporting by the intelligence community of possible criminal activity to the Department of Justice.

REPORTS OF POSSIBLE CRIMINAL ACTIVITY INVOLVING FOREIGN INTELLIGENCE SOURCES GUIDELINES

After conferencing with the referencing agency, receiving any necessary additional information, and consulting with other appropriate Department components, the Assistant Attorney General or the designated Deputy Assistant Attorney General of the Criminal Division or another appropriate Department attorney shall inform the referring agency within a reasonable period of time whether the Department intends to commence or decline to commence a criminal investigation of the conduct described in the crime report. In all cases, Department attorneys shall take into account any special time urgency associated with the intelligence community agency's intelligence equities or the possible criminal activity and, if necessary, provide notice of the prosecutorial decision on a highly expedited basis. Except in extraordinary circumstances, the referencing agency should be informed within 30 days. Extraordinary circumstances requiring more than 30 days may include situations where the case is of unusual complexity or where information necessary for a prosecutorial decision is unavailable.

These procedures are not intended to and do not create any rights, privileges, or benefits, substantive or procedural, enforceable by any party against the United State, its departments, agencies, or other entities, its officers or employees, or any other person.

The guidelines in this memorandum shall be effective immediately.

**GUIDELINES TO ENSURE THAT THE INFORMATION PRIVACY
AND OTHER LEGAL RIGHTS OF AMERICANS ARE PROTECTED
IN THE DEVELOPMENT AND USE OF THE
INFORMATION SHARING ENVIRONMENT**

1. BACKGROUND AND APPLICABILITY.

(a) BACKGROUND. Section 1016(d) of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) calls for the issuance of guidelines to protect privacy and civil liberties in the development and use of the “information sharing environment” (ISE). Section 1 of Executive Order 13388, Further Strengthening the Sharing of Terrorism Information to Protect Americans, provides that, “[t]o the maximum extent consistent with applicable law, agencies shall ... give the highest priority to ... the interchange of terrorism information among agencies ... [and shall] protect the freedom, information privacy, and other legal rights of Americans in the conduct of [such] activities ...” These Guidelines implement the requirements under the IRTPA and EO 13388 to protect information privacy rights and provide other legal protections relating to civil liberties and the legal rights of Americans in the development and use of the ISE.

(b) APPLICABILITY. These Guidelines apply to information about United States citizens and lawful permanent residents that is subject to information privacy or other legal protections under the Constitution and Federal laws of the United States (“protected information”). For the intelligence community, protected information includes information about “United States persons” as defined in Executive Order 12333. Protected information may also include other information that the U.S. Government expressly determines by Executive Order, international agreement, or other similar instrument, should be covered by these Guidelines.

2. COMPLIANCE WITH LAWS.

(a) GENERAL. In the development and use of the ISE, all agencies shall, without exception, comply with the Constitution and all applicable laws and Executive Orders relating to protected information.

(b) RULES ASSESSMENT. Each agency shall implement an ongoing process for identifying and assessing the laws, Executive Orders, policies, and procedures that apply to the protected information that it will make available or access through the ISE. Each agency shall identify, document, and comply with any legal restrictions applicable to such information. Each agency shall adopt internal policies and procedures requiring it to:

(i) only seek or retain protected information that is legally permissible for the agency to seek or retain under the laws, regulations, policies, and executive orders applicable to the agency; and

(ii) ensure that the protected information that the agency makes available through the ISE has been lawfully obtained by the agency and may be lawfully made available through the ISE.

(c) CHANGES. If, as part of its rules assessment process, an agency:

(i) identifies an issue that poses a significant risk to information privacy rights or other legal protections, it shall as appropriate develop policies and procedures to provide protections that address that issue;

(ii) identifies a restriction on sharing protected information imposed by internal agency policy, that significantly impedes the sharing of terrorism information, homeland security information, or law enforcement information (as defined in Section 13 below) in a manner that does not appear to be required by applicable laws or to protect information privacy rights or provide other legal protections, it shall review the advisability of maintaining such restriction;

(iii) identifies a restriction on sharing protected information, other than one imposed by internal agency policy, that significantly impedes the sharing of information in a manner that does not appear to be required to protect information privacy rights or provide other legal protections, it shall review such restriction with the ISE Privacy Guidelines Committee (described in Section 12 below), and if an appropriate internal resolution cannot be developed, bring such restriction to the attention of the Attorney General and the Director of National Intelligence (DNI). The Attorney General and the DNI shall review any such restriction and jointly submit any recommendations for changes to such restriction to the Assistant to the President for Homeland Security and Counterterrorism, the Assistant to the President for National Security Affairs, and the Director of the Office of Management and Budget for further review.

3. PURPOSE SPECIFICATION. Protected information should be shared through the ISE only if it is terrorism information, homeland security information, or law enforcement information (as defined in Section 13 below). Each agency shall adopt internal policies and procedures requiring it to ensure that the agency's access to and use of protected information available through the ISE is consistent with the authorized purpose of the ISE.

4. IDENTIFICATION OF PROTECTED INFORMATION TO BE SHARED THROUGH THE ISE.

(a) IDENTIFICATION AND PRIOR REVIEW. In order to facilitate compliance with these Guidelines, particularly Section 2 (Compliance with Laws) and Section 3 (Purpose Specification), each agency shall identify its data holdings that contain protected information to be shared through the ISE, and shall put in place such

mechanisms as may be reasonably feasible to ensure that protected information has been reviewed pursuant to these Guidelines before it is made available to the ISE.

(b) **NOTICE MECHANISMS.** Consistent with guidance and standards to be issued for the ISE, each agency shall put in place a mechanism for enabling ISE participants to determine the nature of the protected information that the agency is making available to the ISE, so that such participants can handle the information in accordance with applicable legal requirements. Specifically, such a mechanism will, to the extent reasonably feasible and consistent with the agency's legal authorities and mission requirements, allow for ISE participants to determine whether:

- (i) the information pertains to a United States citizen or lawful permanent resident;
- (ii) the information is subject to specific information privacy or other similar restrictions on access, use or disclosure, and if so, the nature of such restrictions; and
- (iii) there are limitations on the reliability or accuracy of the information.

5. DATA QUALITY.

(a) **ACCURACY.** Each agency shall adopt and implement procedures, as appropriate, to facilitate the prevention, identification, and correction of any errors in protected information with the objective of ensuring that such information is accurate and has not erroneously been shared through the ISE.

(b) **NOTICE OF ERRORS.** Each agency, consistent with its legal authorities and mission requirements, shall ensure that when it determines that protected information originating from another agency may be erroneous, includes incorrectly merged information, or lacks adequate context such that the rights of the individual may be affected, the potential error or deficiency will be communicated in writing to the other agency's ISE privacy official (the ISE privacy officials are described in section 12 below).

(c) **PROCEDURES.** Each agency, consistent with its legal authorities and mission requirements, shall adopt and implement policies and procedures with respect to the ISE requiring the agency to:

- (i) take appropriate steps, when merging protected information about an individual from two or more sources, to ensure that the information is about the same individual;
- (ii) investigate in a timely manner alleged errors and deficiencies and correct, delete, or refrain from using protected information found to be erroneous or deficient; and
- (iii) retain protected information only so long as it is relevant and timely for appropriate use by the agency, and update, delete, or refrain from

using protected information that is outdated or otherwise irrelevant for such use.

6. **DATA SECURITY.** Each agency shall use appropriate physical, technical, and administrative measures to safeguard protected information shared through the ISE from unauthorized access, disclosure, modification, use, or destruction.

7. **ACCOUNTABILITY, ENFORCEMENT AND AUDIT.**

(a) **PROCEDURES.** Each agency shall modify existing policies and procedures or adopt new ones as appropriate, requiring the agency to:

(i) have and enforce policies for reporting, investigating, and responding to violations of agency policies relating to protected information, including taking appropriate action when violations are found;

(ii) provide training to personnel authorized to share protected information through the ISE regarding the agency's requirements and policies for collection, use, and disclosure of protected information, and, as appropriate, for reporting violations of agency privacy protection policies;

(iii) cooperate with audits and reviews by officials with responsibility for providing oversight with respect to the ISE; and

(iv) designate each agency's ISE privacy official to receive reports (or copies thereof if the agency already has a designated recipient of such reports) regarding alleged errors in protected information that originate from that agency.

(b) **AUDIT.** Each agency shall implement adequate review and audit mechanisms to enable the agency's ISE privacy official and other authorized officials to verify that the agency and its personnel are complying with these Guidelines in the development and use of the ISE.

8. **REDRESS.** To the extent consistent with its legal authorities and mission requirements, each agency shall, with respect to its participation in the development and use of the ISE, put in place internal procedures to address complaints from persons regarding protected information about them that is under the agency's control.

9. **EXECUTION, TRAINING, AND TECHNOLOGY.**

(a) **EXECUTION.** The ISE privacy official shall be responsible for ensuring that protections are implemented as appropriate through efforts such as training, business process changes, and system designs.

(b) **TRAINING.** Each agency shall develop an ongoing training program in the implementation of these Guidelines, and shall provide such training to agency personnel participating in the development and use of the ISE.

(c) **TECHNOLOGY.** Where reasonably feasible, and consistent with standards and procedures established for the ISE, each agency shall consider and implement, as appropriate, privacy enhancing technologies including, but not limited to, permissioning systems, hashing, data anonymization, immutable audit logs, and authentication.

10. **AWARENESS.** Each agency shall take steps to facilitate appropriate public awareness of its policies and procedures for implementing these Guidelines.

11. **NON-FEDERAL ENTITIES.** Consistent with any standards and procedures that may be issued to govern participation in the ISE by State, tribal, and local governments and private sector entities, the agencies and the PM-ISE will work with non-Federal entities seeking to access protected information through the ISE to ensure that such non-Federal entities develop and implement appropriate policies and procedures that provide protections that are at least as comprehensive as those contained in these Guidelines.

12. **GOVERNANCE.**

(a) **ISE PRIVACY OFFICIALS.** Each agency's senior official with overall agency-wide responsibility for information privacy issues (as designated by statute or executive order, or as otherwise identified in response to OMB Memorandum M-05-08 dated February 11, 2005), shall directly oversee the agency's implementation of and compliance with these Guidelines (the "ISE privacy official"). If a different official would be better situated to perform this role, he or she may be so designated by the head of the agency. The ISE privacy official role may be delegated to separate components within an agency, such that there could be multiple ISE privacy officials within one executive department. The ISE privacy official shall be responsible for ensuring that (i) the agency's policies, procedures, and systems are appropriately designed and executed in compliance with these Guidelines, and (ii) changes are made as necessary. The ISE privacy official should be familiar with the agency's activities as they relate to the ISE, possess all necessary security clearances, and be granted the authority and resources, as appropriate, to identify and address privacy and other legal issues arising out of the agency's participation in the ISE. Such authority should be exercised in coordination with the agency's senior ISE official.

(b) **ISE PRIVACY GUIDELINES COMMITTEE.** All agencies will abide by these Guidelines in their participation in the ISE. The PM shall establish a standing "ISE Privacy Guidelines Committee" to provide ongoing guidance on the

implementation of these Guidelines, so that, among other things, agencies follow consistent interpretations of applicable legal requirements, avoid duplication of effort, share best practices, and have a forum for resolving issues on an inter-agency basis. The ISE Privacy Guidelines Committee is not intended to replace legal or policy guidance mechanisms established by law, executive order, or as part of the ISE, and will as appropriate work through or in consultation with such other mechanisms. The ISE Privacy Guidelines Committee shall be chaired by the PM or a senior official designated by the PM, and will consist of the ISE privacy officials of each member of the Information Sharing Council. If an issue cannot be resolved by the ISE Privacy Guidelines Committee, the PM will address the issue through the established ISE governance process. The ISE Privacy Guidelines Committee should request legal or policy guidance on questions relating to the implementation of these Guidelines from those agencies having responsibility or authorities for issuing guidance on such questions; any such requested guidance shall be provided promptly by the appropriate agencies. As the ISE governance process evolves, if a different entity is established or identified that could more effectively perform the functions of the ISE Privacy Guidelines Committee, the ISE Privacy Guidelines Committee structure shall be modified by the PM through such consultation and coordination as may be required by the ISE governance process, to ensure the functions and responsibilities of the ISE Privacy Guidelines Committee remain priorities fully integrated into the overall ISE governance process.

(c) **PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD.** The Privacy and Civil Liberties Oversight Board (PCLOB) should be consulted for ongoing advice regarding the protection of privacy and civil liberties in agencies' development and use of the ISE. To facilitate the performance of the PCLOB's duties, the ISE Privacy Guidelines Committee will serve as a mechanism for the PCLOB to obtain information from agencies and to provide advice and guidance consistent with the PCLOB's statutory responsibilities. Accordingly, the ISE Privacy Guidelines Committee should work in consultation with the PCLOB, whose members may attend Committee meetings, provide advice, and review and comment on guidance as appropriate.

(d) **ISE PRIVACY PROTECTION POLICY.** Each agency shall develop and implement a written ISE privacy protection policy that sets forth the mechanisms, policies, and procedures its personnel will follow in implementing these Guidelines. Agencies should consult with the ISE Privacy Guidelines Committee as appropriate in the development and implementation of such policy.

13. GENERAL PROVISIONS.

(a) DEFINITIONS.

(i) The term “agency” has the meaning set forth for the term “executive agency” in section 105 of title 5, United States Code, but includes the Postal Rate Commission and the United States Postal Service and excludes the Government Accountability Office.

(ii) The term “protected information” has the meaning set forth for such term in paragraph 1(b) of these Guidelines.

(iii) The terms “terrorism information,” “homeland security information,” and “law enforcement information” are defined as follows:

[I] “Terrorism information,” consistent with section 1016(a)(4) of IRTPA means all relating to (A) the existence, organization, capabilities, plans, intentions, vulnerabilities, means of finance or material support, or activities of foreign or international terrorist groups or individuals, or of domestic groups or individuals involved in transnational terrorism, (B) threats posed by such groups or individuals to the United States, United States persons, or United States interests, or to those of other nations, (C) communications of or by such groups or individuals, or (D) groups or individuals reasonably believed to be assisting or associated with such groups or individuals.

[II] “Homeland security information,” as derived from section 482(f)(1) of the Homeland Security Act of 2002, means any information possessed by a Federal, State, local, or tribal agency that relates to (A) a threat of terrorist activity, (B) the ability to prevent, interdict, or disrupt terrorist activity, (C) the identification or investigation of a suspected terrorist or terrorist organization or any person, group, or entity associated with or assisting a suspected terrorist or terrorist organization, or (D) a planned or actual response to a terrorist act.

[III] “Law enforcement information” for the purposes of the ISE means any information obtained by or of interest to a law enforcement agency or official that is (A) related to terrorism or the security of our homeland and (B) relevant to a law enforcement mission, including but not limited to information pertaining to an actual or potential criminal, civil, or administrative investigation or a foreign intelligence, counterintelligence, or counterterrorism investigation; assessment of or response to criminal threats and vulnerabilities; the existence, organization, capabilities, plans, intentions, vulnerabilities, means, methods, or activities of individuals or groups involved or suspected of involvement in

criminal or unlawful conduct or assisting or associated with criminal or unlawful conduct; the existence, identification, detection, prevention, interdiction, or disruption of, or response to, criminal acts and violations of the law; identification, apprehension, prosecution, release, detention, adjudication, supervision, or rehabilitation of accused persons or criminal offenders; and victim/witness assistance.

- (b) The treatment of information as “protected information” under these Guidelines does not by itself establish that the individual or entity to which such information pertains does in fact have information privacy or other legal rights with respect to such information.
- (c) Heads of executive departments and agencies shall, to the extent permitted by law and subject to the availability of appropriations, provide the cooperation, assistance, and information necessary for the implementation of these Guidelines.
- (d) These Guidelines:
- (i) shall be implemented in a manner consistent with applicable laws and executive orders, including Federal laws protecting the information privacy rights and other legal rights of Americans, and subject to the availability of appropriations;
 - (ii) shall be implemented in a manner consistent with the statutory authority of the principal officers of executive departments and agencies as heads of their respective departments or agencies;
 - (iii) shall not be construed to impair or otherwise affect the functions of the Director of the Office of Management and Budget relating to budget, administrative, and legislative proposals; and
 - (iv) are intended only to improve the internal management of the Federal Government and are not intended to, and do not, create any rights or benefits, substantive or procedural, enforceable at law or in equity by a party against the United States, its departments, agencies, or entities, its officers, employees, or agencies, or any other person.

IMPROVING CYBERSECURITY MEMORANDUM

MEMORANDUM ON IMPROVING THE CYBERSECURITY OF
NATIONAL SECURITY, DEPARTMENT OF DEFENSE, AND
INTELLIGENCE COMMUNITY SYSTEMS

THE WHITE HOUSE

January 19, 2022

NATIONAL SECURITY MEMORANDUM/NSM-8

SUBJECT: Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems

This memorandum sets forth requirements for National Security Systems (NSS) that are equivalent to or exceed the cybersecurity requirements for Federal Information Systems set forth within Executive Order 14028 of May 12, 2021 (Improving the Nation's Cybersecurity), and establishes methods to secure exceptions for circumstances necessitated by unique mission needs. Executive Order 14028 establishes that the Federal Government must improve its efforts to identify, deter, protect against, detect, and respond to malicious cyber campaigns and their actors through bold changes and significant investments in cybersecurity. This memorandum establishes and clarifies additional authority and responsibilities of the Director of the National Security Agency (NSA) in connection with the National Manager responsibilities for NSS assigned to the Director of the NSA by National Security Directive 42 of July 5, 1990 (National Policy for the Security of National Security Telecommunications and Information Systems) (NSD-42), Executive Order 12333 of December 4, 1981, as amended (United States Intelligence Activities), and Executive Order 14028.

Consistent with Executive Order 14028, NSS shall include those systems defined as NSS in 44 U.S.C. 3552(b)(6) as well as all other Department of Defense and Intelligence Community systems, as described in 44 U.S.C. 3553(e)(2) and 3553(e)(3).

Section 1. Implementation of Executive Order 14028 for National Security Systems.

(a) Sections 1 and 2 of Executive Order 14028 shall apply in their entirety to NSS, except that the authorities exercised by the Director of the Office of Management and Budget and the Secretary of Homeland Security in section 2 shall be exercised by the National Manager with respect to NSS.

(b) Consistent with section 3 of Executive Order 14028:

IMPROVING CYBERSECURITY MEMORANDUM

- (i) Within 90 days of the date of this memorandum, the Committee on National Security Systems (CNSS) shall develop and publish guidance, in addition to CNSS Instruction (CNSSI) 1253, regarding minimum security standards and controls related to cloud migration and operations for NSS, taking into account migration steps that the National Institute of Standards and Technology (NIST) within the Department of Commerce has outlined in standards and guidance.
- (ii) Within 60 days of the date of this memorandum, the head of each executive department or agency (agency) that owns or operates an NSS shall, consistent with its statutory authority:
- (A) update existing agency plans to prioritize resources for the adoption and use of cloud technology, including adoption of Zero Trust Architecture as practicable;
 - (B) develop a plan to implement Zero Trust Architecture, which shall incorporate, as appropriate:
 - (1) NIST Special Publication 800-207 Guidance (Zero Trust Architecture);
 - (2) CNSS instructions on Zero Trust Reference Architectures; and
 - (3) Other relevant CNSS instructions, directives, and policies regarding enterprise architectures, insider threats, and access management; and
 - (C) provide a report to the CNSS and National Manager discussing the plans required pursuant to section 1(b)(ii)(A) and (B) of this memorandum.
- (iii) Within 180 days of the date of this memorandum, agencies shall implement multifactor authentication and encryption for NSS data-at-rest and data-in-transit. In those instances where the head of an agency determines the agency is unable to implement these measures, the head of the agency shall authorize an exception pursuant to the process provided in section 3 of this memorandum.
- (iv) To ensure widespread cryptographic interoperability among NSS, all agencies shall use NSA-approved, public standards-based cryptographic protocols. If mission-unique requirements preclude the use of public standards-based cryptographic protocols, NSA-approved mission unique protocols may be used. An agency shall not authorize new systems to operate that do not use approved encryption algorithms and implementations, absent an exception authorized by the head of an agency pursuant to section 3 of this memorandum.
- (A) Within 30 days of the date of this memorandum, the NSA shall review CNSS Policy 15 and provide to CNSS any updates or

IMPROVING CYBERSECURITY MEMORANDUM

modifications regarding the approved list of commercial national security algorithms (CNSA).

(B) Within 60 days of the date of this memorandum, the NSA shall revise and make available to Chief Information Officers the CNSS Advisory Memorandum 01-07 (Information Assurance Cryptographic Equipment Modernization) and any associated enclosures and relevant references regarding modernization planning, use of unsupported encryption, approved mission unique protocols, quantum resistant protocols, and planning for use of quantum resistant cryptography where necessary.

(C) Within 90 days of the date of this memorandum, CNSS shall identify and prioritize for update all cryptographic-related policies, directives, and issuances, and CNSS shall provide to the Secretary of Defense, the Director of National Intelligence, and the National Manager a timeline, not to exceed 6 months, for the re-issuance of these policies, as appropriate.

(D) Within 180 days of the date of this memorandum, agencies shall identify any instances of encryption not in compliance with NSA-approved Quantum Resistant Algorithms or CNSA, where appropriate in accordance with section 1(b)(iv)(A) and (B) of this memorandum, and shall report to the National Manager, at a classification level not to exceed TOP SECRET//SI//NOFORN:

- (1) systems where non-compliant encryption is being used, to include those operating under an existing waiver or exception;
- (2) a timeline to transition these systems to use compliant encryption, to include quantum resistant encryption; and
- (3) any exception from transition to compliant encryption, pursuant to section 3 of this memorandum, which shall additionally be reviewed by the National Manager and reported quarterly to the Secretary of Defense and the Director of National Intelligence for the systems within their respective jurisdictions. The National Manager, in coordination with and only after engaging the system owner, may include other relevant agencies if a shared risk is jointly determined.

(v) Within 90 days of the date of this memorandum, the National Manager shall, in coordination with the Director of National Intelligence, the Director of the Central Intelligence Agency, the Director of the Federal Bureau of Investigation, and the heads of appropriate elements of the Department of Defense, develop a framework to coordinate and collaborate on cybersecurity and incident response activities related to NSS commercial cloud technologies that ensures effective information

IMPROVING CYBERSECURITY MEMORANDUM

sharing among agencies, the National Manager, and Cloud Service Providers (CSP).

(A) The National Manager, in coordination with the Secretary of Homeland Security, shall ensure that, as provided in the framework, there is a Federal unity of effort and collaboration between the Secretary of Homeland Security and the National Manager on commercial CSP-cybersecurity and incident management, consistent with each agency's responsibilities for Federal Civilian Executive Branch (FCEB) and NSS cybersecurity, and to ensure rapid and thorough end-to-end risk mitigation across CSP environments.

(B) The National Manager shall ensure that the final version of the framework is coordinated with the Director of National Intelligence, the Director of the Central Intelligence Agency, the Director of the Federal Bureau of Investigation, and the heads of appropriate elements of the Department of Defense.

(c) Consistent with section 4 of Executive Order 14028:

(i) Except as otherwise authorized by law, or by an exception authorized by the heads of agencies pursuant to section 3 of this memorandum, agencies shall adhere to the standards developed under section 4 of Executive Order 14028 for any software intended to be used on NSS for which this category of software is applicable.

(ii) Within 60 days of the date of this memorandum, the National Manager shall, in coordination with the Secretary of Defense and the Director of National Intelligence, review the guidance issued by the Office of Management and Budget pursuant to section 4(i) of Executive Order 14028 and shall issue similar guidance.

(iii) Agencies may request from the National Manager an extension to the time period associated with satisfaction of the applicable requirements issued in section 1(c)(ii) of this memorandum, which will be considered by the National Manager on a case-by-case basis and only with an accompanying plan for satisfying requirements. The National Manager shall provide a quarterly report to the Secretary of Defense and the Director of National Intelligence of all extensions granted for the systems within their respective jurisdictions and the justifications for doing so. The National Manager, in coordination with and only after engaging the system owner, may include other relevant agencies if a shared risk is jointly determined.

(d) Section 6 of Executive Order 14028 shall apply to NSS owners and operators, utilizing the National Manager to review and validate agencies' incident response and remediation results upon an agency's completion of its incident response pursuant to section 6(f) of Executive Order 14028.

IMPROVING CYBERSECURITY MEMORANDUM

(e) Section 7 of Executive Order 14028 shall apply to NSS owners and operators where specifically referenced within the Executive Order, with additional requirements as described in section 2(b) of this memorandum.

(f) Within 14 days of the date of this memorandum the National Manager, in coordination with the Secretary of Defense and the Director of National Intelligence, shall provide to the CNSS recommendations as described in section 8(b) of Executive Order 14028.

(i) Within 90 days of receipt of the recommendations issued pursuant to section 1(f) of this memorandum, the CNSS shall formulate policies for agencies to establish such requirements, which shall ensure centralized access and visibility for the highest level of security operations center of each agency.

(ii) To assist in the response to known or suspected compromise of an NSS, recommendations issued pursuant to section 1(f) of this memorandum shall include requirements that agencies will allow access, upon request, to logs by specified named individuals, or based on specific NSA cyber defense mission roles, as agreed upon between the National Manager and the head of the agency or designee.

Sec. 2. National Manager Authorities Relating to National Security Systems.

(a) Designation and Identification of National Security Systems.

(i) The National Manager shall facilitate the designation of NSS across the Federal Government. Each agency shall remain responsible for identification, designation, accreditation, and protection of all NSS under its ownership or control, including those NSS operated and/or maintained on behalf of the agency. The National Manager may, on a periodic basis, request access to NSS information regarding the designation and identification of such systems from agencies operating NSS.

(ii) Within 30 days of the date of this memorandum, the National Manager shall develop a process for assisting agencies with identifying and inventorying those information systems that do or should likely constitute NSS, and shall issue guidance to support agencies in making these determinations to agency Chief Information Officers. NSS shall be inventoried at a level of detail sufficient to understand community-wide cybersecurity risk, as determined by the National Manager, and such information may not exceed a classification level of TOP SECRET//SI//NOFORN.

(iii) Within 90 days of the date of this memorandum, agencies shall identify and maintain an inventory of those systems designated as NSS through the process designated in section 2(a)(ii) of this memorandum. Agencies shall retain their own inventory subject to access by specified

IMPROVING CYBERSECURITY MEMORANDUM

named individuals, or based on specific NSA cyber defense mission roles, as agreed upon between the National Manager and the head of the agency or designee.

(iv) If the National Manager has concerns regarding the determination as to whether a system constitutes an NSS, the National Manager shall engage the head of the relevant agency in order to resolve the designation. If the National Manager and the head of the agency are unable to achieve a mutually acceptable resolution, the National Manager may request that the head of the agency report the disagreement to the Secretary of Defense and the Director of National Intelligence for further consideration for systems within their respective jurisdictions. The National Manager, in coordination with and only after engaging the system owner, may include other relevant agencies if a shared risk is jointly determined.

(v) Once a system has been identified and designated as an NSS, notification to the National Manager and to the Secretary of Defense and the Director of National Intelligence, for systems within their respective jurisdictions, will be required to re-designate those systems as non-NSS. The National Manager, in coordination with and only after engaging the system owner, may include other relevant agencies if a shared risk is jointly determined.

(b) Incident Reporting.

(i) To facilitate threat detection and response, as well as an overall understanding of the cybersecurity status of NSS, an agency shall, upon agency detection, or upon report by a contractor (including an information and communications technology service provider) or other Federal or non-Federal entity, of a known or suspected compromise or otherwise unauthorized access to NSS, report such compromise or unauthorized access to the National Manager through the appropriate Federal Cyber Center or other designated central department point of contact. Agencies shall also provide relevant information to the National Manager pursuant to the policies developed in accordance with section 1(f) of this memorandum.

(ii) Agencies shall, upon detection or report to the agency, also report to the National Manager, through their appropriate Federal Cyber Center or other designated central department point of contact, any compromise or unauthorized access of a network hosting a Cross Domain Solution (CDS) when one side of the CDS connects to NSS operated by or on behalf of the agency.

(iii) Within 90 days of the date of this memorandum, the National Manager, in coordination with the Director of National Intelligence and

IMPROVING CYBERSECURITY MEMORANDUM

the Director of the Central Intelligence Agency, shall establish procedures for reporting known or suspected compromises of NSS or otherwise unauthorized access of NSS, which shall include:

- (A) thresholds, required information, and other criteria;
- (B) emergency procedures if an imminent threat to NSS is detected;
- (C) timeliness expectations regarding initiation of response activities by the affected agency;
- (D) threat and compromise reporting mechanisms between the National Manager and affected agencies;
- (E) expectations of the National Manager's protection and handling of any information received pursuant to this section, to include any considerations regarding the protection of intelligence sources and methods and the conduct of counterintelligence investigations;
- (F) expectations for advising the Secretary of Defense and the Director of National Intelligence for systems within their respective jurisdictions of instances where agencies have failed to report a known or suspected compromise of NSS; and
- (G) procedures for the National Manager, in coordination with and only after engaging the system owner, to include other relevant agencies if a shared risk is jointly determined.

(iv) The recipients of any reporting required by this section may be limited to specified named individuals or, based on specific NSA cyber defense mission roles, as agreed upon between the National Manager and the head of the agency or designee. In exceptional cases where the head of the agency deems it advisable to limit reporting in order to protect intelligence sources and methods, counterintelligence investigations, or law enforcement sensitive information, the reporting may be retained by the agency subject to the National Manager access described in section 2(a)(iii) of this memorandum.

(c) National Manager Directives.

(i) Emergency Directives. In response to a known or reasonably suspected information security threat, vulnerability, or incident that represents a substantial threat to the information security of NSS, or intelligence of adversary capability and intent to target NSS, the National Manager may issue a National Manager Emergency Directive to the head of an agency, through that agency's Chief Information Officer, Chief Information Security Officer, or officer designated by the head of the agency, to take any lawful action with respect to the operation of that NSS, as defined in this memorandum, including such systems used or operated by another entity on behalf of an agency, for the purpose of protecting the NSS from, or mitigating, the threat, vulnerability, or risk.

IMPROVING CYBERSECURITY MEMORANDUM

(ii) Binding Operational Directives. For the purposes of safeguarding NSS from a known or reasonably suspected information security threat, vulnerability, or risk, the National Manager may, in coordination with the Secretary of Defense and the Director of National Intelligence, for the systems within their respective jurisdictions, issue a National Manager Binding Operational Directive to the head of an agency, through that agency's Chief Information Officer, Chief Information Security Officer, or officer designated by the head of the agency, to take any lawful action with respect to the operation of that NSS, as defined in this memorandum, including such systems used or operated by another entity on behalf of an agency, for the purpose of protecting the NSS from, or mitigating, the threat, vulnerability, or risk. Additionally, the National Manager may issue, on a periodic or ad hoc basis, requests to the head of an agency, through that agency's Chief Information Officer, Chief Information Security Officer, or officer designated by the head of the agency, for information suitable for reporting the overall cybersecurity posture of that agency's NSS.

(iii) Implementing Procedures. Within 30 days of the date of this memorandum, the National Manager, in coordination with the Secretary of Defense and the Director of National Intelligence, shall establish procedures governing the circumstances under which a directive may be issued under this subsection, which shall include:

- (A) thresholds and other criteria;
- (B) provision of notice to potentially affected third parties;
- (C) reasons for the required action and the duration of the directive;
- (D) privacy and civil liberties protections;
- (E) adoption of measures to secure the NSS that have a minimal impact on operations under the circumstances; and
- (F) limiting directives to the shortest period practicable.

(iv) Notification and Assistance. The National Manager shall notify, in writing, the head of any affected agency, the Secretary of Defense, the Secretary of Homeland Security, and the Director of National Intelligence immediately upon the issuance of an Emergency Directive or Binding Operational Directive, and shall provide technical and operational assistance to the implementing agency.

(v) Coordination and Alignment of Directives. To ensure alignment between National Manager directives for NSS and FCEB information systems directives, the National Manager and the Secretary of Homeland Security, in coordination with the Secretary of Defense and the Director of National Intelligence, shall:

IMPROVING CYBERSECURITY MEMORANDUM

(A) within 60 days of the date of this memorandum, establish procedures for the National Manager and the Secretary of Homeland Security to immediately share with each other National Manager Binding Operational Directives and Emergency Directives, and Department of Homeland Security Emergency Directives and Binding Operational Directives, applying to the information networks within their respective jurisdictions. The procedures shall adequately address applicable information-sharing guidelines, including protections for classified information, protection of intelligence sources and methods, and protection of information originated by other agencies;

(B) evaluate whether to adopt any requirements or guidance contained in a directive received pursuant to the procedures established under section 2(c)(v)(A) of this memorandum, consistent with law, Executive Orders, Federal regulations, and directives concerning the sharing of classified information; and

(C) within 7 days of receiving notice of a directive issued pursuant to the procedures established under section 2(c)(v)(A) of this memorandum, notify the Assistant to the President for National Security Affairs (APNSA) or their designee of the evaluation described in section 2(c)(v)(B) of this memorandum, the determination of whether to adopt the requirements or guidance contained in the directive received, the rationale for that determination, and a timeline for adoption of the requirements or guidance, if applicable.

(d) Cross Domain Solutions.

(i) As CDS separate and enable controlled exchange of information between different security domains, they are vital NSS that require centralized visibility.

(ii) In operating the National Cross Domain Strategy and Management Office (NCDSMO), the National Manager shall be the focal point for NSS cross domain capabilities and mission needs, and shall:

(A) serve as the principal advisor to NSS owners for cross domain capabilities;

(B) develop and maintain community outreach programs and forums;

(C) develop and establish improved security solutions, remote management and monitoring, cyber defense, filtering requirements, and standards and technologies for CDS; and

(D) operate the cross domain security testing program to ensure uniform comprehensive testing.

IMPROVING CYBERSECURITY MEMORANDUM

(iii) Within 60 days of the date of this memorandum, the National Manager, in coordination with the Chief Information Officer of the Intelligence Community, shall issue a directive to all agencies operating a CDS connected to NSS to make available information regarding those deployments and shall establish timelines for the collection and receipt of this information, requiring that agencies shall:

(A) verify that logs from CDS, supporting systems, and connected systems are collected and archived by agencies, sufficient to support investigation and incident response activities, as well as ensuring the logs are intact and machine-readable, and making access to that information available to the National Manager consistent with section 2(b) of this memorandum;

(B) validate that the latest authorized patches have been installed for deployed CDS;

(C) report on the status of upgrading to the Raise-the-Bar (RTB) compliant version of their CDS; and

(D) update or develop plans of actions and milestones for all CDS installations to comply with NCDSMO CDS security requirements and provide these plans to the National Manager, to include identified funding barriers which may prevent RTB compliance.

(iv) Within 90 days of the date of this memorandum, the heads of relevant agencies shall establish and maintain CDS deployment inventory for all CDS deployments within their jurisdiction, subject to access by specified named individuals, or based on specific NSA cyber defense mission roles, as agreed upon between the National Manager and the head of the agency or designee. In coordination with the Secretary of Defense and the Director of National Intelligence, the National Manager shall define essential elements of information required to maintain an accurate inventory not to exceed a classification level of TOP SECRET//SI//NOFORN, shall define initial and ongoing agency reporting expectations, and shall provide a process to CDS owners for reporting and updating as required.

Sec. 3. Exceptions.

(a) Whenever the head of an agency determines that unique mission needs necessitate any NSS or category of NSS to be excepted from any provisions of Executive Order 14028 or this memorandum, the head of the agency may authorize such exceptions, provided that such exceptions may only be authorized with respect to:

(i) systems that facilitate the support or conduct of military, intelligence, or sensitive law enforcement activities where the head of the

IMPROVING CYBERSECURITY MEMORANDUM

agency determines that implementation of these requirements is not practicable or is contrary to national security;

(ii) systems for which attribution to the United States Government is obscured and for which this attribution would be reasonably endangered due to implementation of these requirements; or

(iii) information systems or software procured for vulnerability research, testing, or evaluation purposes that are not intended for use in agency operational networks.

(b) If the head of an agency elects to authorize an exception under section 3(a) of this memorandum, the head of the agency shall notify the National Manager and shall provide:

(i) a general description as to the function of the system or systems at issue;

(ii) the reasoning for accepting the enhanced cybersecurity risk resulting from the exception;

(iii) a description of the likely mission impact, and agency response, were this NSS to be compromised; and

(iv) attestation that all practicable means of risk mitigation have been, or will be, implemented.

(c) In order to ensure that the National Manager maintains awareness of additional cybersecurity risk across NSS, the National Manager, in coordination with the Secretary of Defense and the Director of National Intelligence, shall, within 30 days of the date of this memorandum:

(i) publish an exception provision process to include: reporting timeline expectations; formats; allowance for categories of systems that may be grouped together within a single exception; and other required elements of information, to include those elements described in section 3(b) of this memorandum. Exceptions shall be sufficiently detailed to establish and maintain an appropriate level of community-wide risk awareness and appropriately abridged to protect sensitive intelligence sources or methods, and classification shall not exceed TOP SECRET//SI//NOFORN; and

SECRET//SI//NOFORN; and

(ii) coordinate with agencies to establish an authoritative repository for each agency to maintain a consolidated inventory of all exceptions that agency has authorized, subject to access by specified named individuals or based on specific NSA cyber defense mission roles, as agreed upon between the National Manager and the head of the agency or designee.

(d) Chief Information Officers of agencies shall retain internal records regarding system exceptions sufficiently detailed to perform effective and timely identification and mitigation of any cybersecurity issues that may impact these systems.

IMPROVING CYBERSECURITY MEMORANDUM

(e) If the National Manager and the head of an agency cannot agree on the sufficiency of exception rationale, description of impacts, response, sufficiency of mitigations, or overall acceptance of increased risk, the National Manager shall request that the head of the agency report the disparity to the Secretary of Defense and the Director of National Intelligence for further consideration with respect to systems within their respective jurisdictions. The National Manager, in coordination with and only after engaging the system owner, may include other relevant agencies if a shared risk is jointly determined.

Sec. 4. Summary of NSS Policy Creation or Adjustment Actions. Within 90 days of the date of this memorandum, the CNSS, in consultation with the National Manager, shall review this memorandum and deliver to the APNSA a summary of NSS policy creation or adjustment actions and their timeline for implementation. This summary will include any additional items not previously directed within this memorandum to the National Manager or agencies.

Sec. 5. General Provisions.

(a) This memorandum is intended to supplement NSD-42.

(b) Nothing in this memorandum shall be construed to alter or supersede:

(i) the authority granted by law to an executive department or agency, or the head thereof, to include the protection of intelligence sources and methods; or

(ii) the functions of the Director of the Office of Management and Budget relating to budgetary, administrative, or legislative proposals.

(c) Nothing in this memorandum confers the authority to interfere with or to direct a counterintelligence, personnel, criminal, or national security investigation, arrest, search, seizure, or disruption operation or to alter a legal restriction that requires an agency to protect information learned in the course of a counterintelligence, personnel, criminal, or national security investigation.

(d) This memorandum shall be implemented in a manner consistent with applicable law and shall be subject to the availability of appropriations. No implementation measures shall impede the conduct or support of intelligence activities, and all such implementation measures shall be designed to protect intelligence sources and methods.

(e) This memorandum is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

JOSEPH R. BIDEN JR.

TITLE 44, SECTION 3520, UNITED STATES CODE

CHIEF DATA OFFICERS

SECTION 3520.

- (a) **ESTABLISHMENT.**-The head of each agency shall designate a nonpolitical appointee employee in the agency as the Chief Data Officer of the agency.
- (b) **QUALIFICATIONS.**-The Chief Data Officer of an agency shall be designated on the basis of demonstrated training and experience in data management, governance (including creation, application, and maintenance of data standards), collection, analysis, protection, use, and dissemination, including with respect to any statistical and related techniques to protect and de-identify confidential data.
- (c) **FUNCTIONS.**-The Chief Data Officer of an agency shall-
- (1) be responsible for lifecycle data management;
 - (2) coordinate with any official in the agency responsible for using, protecting, disseminating, and generating data to ensure that the data needs of the agency are met;
 - (3) manage data assets of the agency, including the standardization of data format, sharing of data assets, and publication of data assets in accordance with applicable law;
 - (4) in carrying out the requirements under paragraphs (3) and (5), consult with any statistical official of the agency (as designated under section 314 of title 5);
 - (5) carry out the requirements of the agency under subsections (b) through (d), (f), and (i) of section 3506, section 3507, and section 3511;
 - (6) ensure that, to the extent practicable, agency data conforms with data management best practices;
 - (7) engage agency employees, the public, and contractors in using public data assets and encourage collaborative approaches on improving data use;
 - (8) support the Performance Improvement Officer of the agency in identifying and using data to carry out the functions described in section 1124(a)(2) of title 31;
 - (9) support the Evaluation Officer of the agency in obtaining data to carry out the functions described in section 313(d) of title 5;
 - (10) review the impact of the infrastructure of the agency on data asset accessibility and coordinate with the Chief Information Officer of the agency to improve such infrastructure to reduce barriers that inhibit data asset accessibility;

44 USC 3520 – CHIEF DATA OFFICERS

- (11) ensure that, to the extent practicable, the agency maximizes the use of data in the agency, including for the production of evidence (as defined in section 3561), cybersecurity, and the improvement of agency operations;
- (12) identify points of contact for roles and responsibilities related to open data use and implementation (as required by the Director);
- (13) serve as the agency liaison to other agencies and the Office of Management and Budget on the best way to use existing agency data for statistical purposes (as defined in section 3561); and
- (14) comply with any regulation and guidance issued under subchapter III, including the acquisition and maintenance of any required certification and training.

(d) DELEGATION OF RESPONSIBILITIES.-

(1) IN GENERAL.-To the extent necessary to comply with statistical laws, the Chief Data Officer of an agency shall delegate any responsibility under subsection (c) to the head of a statistical agency or unit (as defined in section 3561) within the agency.

(2) CONSULTATION.-To the extent permissible under law, the individual to whom a responsibility has been delegated under paragraph (1) shall consult with the Chief Data Officer of the agency in carrying out such responsibility.

(3) DEFERENCE.-The Chief Data Officer of the agency shall defer to the individual to whom a responsibility has been delegated under paragraph (1) regarding the necessary delegation of such responsibility with respect to any data acquired, maintained, or disseminated by the agency under applicable statistical law.

(e) REPORTS.-The Chief Data Officer of an agency shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Oversight and Government Reform of the House of Representatives an annual report on the compliance of the agency with the requirements of this subchapter, including information on each requirement that the agency could not carry out and, if applicable, what the agency needs to carry out such requirement.

TITLE 10, SECTION 431, UNITED STATES CODE

**AUTHORITY TO ENGAGE IN COMMERCIAL ACTIVITIES AS SECURITY FOR
INTELLIGENCE COLLECTION ACTIVITIES**

SECTION 431.

- (a) **AUTHORITY.**-The Secretary of Defense, subject to the provisions of this subchapter, may authorize the conduct of those commercial activities necessary to provide security for authorized intelligence collection activities abroad undertaken by the Department of Defense. No commercial activity may be initiated pursuant to this subchapter after December 31, 2024.
- (b) **INTERAGENCY COORDINATION AND SUPPORT.**-Any such activity shall-
- (1) be coordinated with, and (where appropriate) be supported by, the Director of the Central Intelligence Agency; and
 - (2) to the extent the activity takes place within the United States, be coordinated with, and (where appropriate) be supported by, the Director of the Federal Bureau of Investigation.
- (c) **DEFINITIONS.**-In this subchapter:
- (1) The term "commercial activities" means activities that are conducted in a manner consistent with prevailing commercial practices and includes-
 - (A) the acquisition, use, sale, storage and disposal of goods and services;
 - (B) entering into employment contracts and leases and other agreements for real and personal property;
 - (C) depositing funds into and withdrawing funds from domestic and foreign commercial business or financial institutions;
 - (D) acquiring licenses, registrations, permits, and insurance; and
 - (E) establishing corporations, partnerships, and other legal entities.
 - (2) The term "intelligence collection activities" means the collection of foreign intelligence and counterintelligence information.

18 USC 2703 – STORED COMMUNICATIONS ACT

TITLE 18, SECTION 2703, UNITED STATES CODE
(THE “STORED COMMUNICATIONS ACT”)

REQUIRED DISCLOSURE OF CUSTOMER COMMUNICATIONS OR RECORDS

SECTION 2703.

(a) **CONTENTS OF WIRE OR ELECTRONIC COMMUNICATIONS IN ELECTRONIC STORAGE.**-A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures and, in the case of a court-martial or other proceeding under chapter 47 of title 10 (the Uniform Code of Military Justice), issued under section 846 of that title, in accordance with regulations prescribed by the President) by a court of competent jurisdiction. A governmental entity may require the disclosure by a provider of electronic communications services of the contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days by the means available under subsection (b) of this section.

(b) **CONTENTS OF WIRE OR ELECTRONIC COMMUNICATIONS IN A REMOTE COMPUTING SERVICE.**-

(1) A governmental entity may require a provider of remote computing service to disclose the contents of any wire or electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection-

(A) without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures and, in the case of a court-martial or other proceeding under chapter 47 of title 10 (the Uniform Code of Military Justice), issued under section 846 of that title, in accordance with regulations prescribed by the President) by a court of competent jurisdiction; or

(B) with prior notice from the governmental entity to the subscriber or customer if the governmental entity-

(i) uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena; or

(ii) obtains a court order for such disclosure under subsection (d) of this section;

18 USC 2703 – STORED COMMUNICATIONS ACT

except that delayed notice may be given pursuant to section 2705 of this title.

(2) Paragraph (1) is applicable with respect to any wire or electronic communication that is held or maintained on that service-

(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such remote computing service; and

(B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.

(c) RECORDS CONCERNING ELECTRONIC COMMUNICATION SERVICE OR REMOTE COMPUTING SERVICE.-

(1) A governmental entity may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications) only when the governmental entity-

(A) obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures and, in the case of a court-martial or other proceeding under chapter 47 of title 10 (the Uniform Code of Military Justice), issued under section 846 of that title, in accordance with regulations prescribed by the President) by a court of competent jurisdiction;

(B) obtains a court order for such disclosure under subsection (d) of this section;

(C) has the consent of the subscriber or customer to such disclosure;

(D) submits a formal written request relevant to a law enforcement investigation concerning telemarketing fraud for the name, address, and place of business of a subscriber or customer of such provider, which subscriber or customer is engaged in telemarketing (as such term is defined in section 2325 of this title); or

(E) seeks information under paragraph (2).

(2) A provider of electronic communication service or remote computing service shall disclose to a governmental entity the-

(A) name;

(B) address;

(C) local and long distance telephone connection records, or records of session times and durations;

(D) length of service (including start date) and types of service utilized;

18 USC 2703 – STORED COMMUNICATIONS ACT

(E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and
(F) means and source of payment for such service (including any credit card or bank account number),
of a subscriber to or customer of such service when the governmental entity uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena or any means available under paragraph (1).

(3) A governmental entity receiving records or information under this subsection is not required to provide notice to a subscriber or customer.

(d) REQUIREMENTS FOR COURT ORDER.-A court order for disclosure under subsection (b) or (c) may be issued by any court that is a court of competent jurisdiction and shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation. In the case of a State governmental authority, such a court order shall not issue if prohibited by the law of such State. A court issuing an order pursuant to this section, on a motion made promptly by the service provider, may quash or modify such order, if the information or records requested are unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider.

(e) NO CAUSE OF ACTION AGAINST A PROVIDER DISCLOSING INFORMATION UNDER THIS CHAPTER.-No cause of action shall lie in any court against any provider of wire or electronic communication service, its officers, employees, agents, or other specified persons for providing information, facilities, or assistance in accordance with the terms of a court order, warrant, subpoena, statutory authorization, or certification under this chapter.

(f) REQUIREMENT TO PRESERVE EVIDENCE.-

(1) IN GENERAL.-A provider of wire or electronic communication services or a remote computing service, upon the request of a governmental entity, shall take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process.

(2) PERIOD OF RETENTION.-Records referred to in paragraph (1) shall be retained for a period of 90 days, which shall be extended for an additional 90-day period upon a renewed request by the governmental entity.

(g) PRESENCE OF OFFICER NOT REQUIRED.-Notwithstanding section 3105 of this title, the presence of an officer shall not be required for service or execution of a search warrant issued in accordance with this chapter requiring disclosure by a provider of electronic communications service or remote computing service of

18 USC 2703 – STORED COMMUNICATIONS ACT

the contents of communications or records or other information pertaining to a subscriber to or customer of such service.

(h) COMITY ANALYSIS AND DISCLOSURE OF INFORMATION REGARDING LEGAL PROCESS SEEKING CONTENTS OF WIRE OR ELECTRONIC COMMUNICATION.-

(1) DEFINITIONS.-In this subsection-

(A) the term "qualifying foreign government" means a foreign government-

(i) with which the United States has an executive agreement that has entered into force under section 2523; and

(ii) the laws of which provide to electronic communication service providers and remote computing service providers substantive and procedural opportunities similar to those provided under paragraphs (2) and (5); and

(B) the term "United States person" has the meaning given the term in section 2523.

(2) MOTIONS TO QUASH OR MODIFY.-

(A) A provider of electronic communication service to the public or remote computing service, including a foreign electronic communication service or remote computing service, that is being required to disclose pursuant to legal process issued under this section the contents of a wire or electronic communication of a subscriber or customer, may file a motion to modify or quash the legal process where the provider reasonably believes-

(i) that the customer or subscriber is not a United States person and does not reside in the United States; and

(ii) that the required disclosure would create a material risk that the provider would violate the laws of a qualifying foreign government.

Such a motion shall be filed not later than 14 days after the date on which the provider was served with the legal process, absent agreement with the government or permission from the court to extend the deadline based on an application made within the 14 days. The right to move to quash is without prejudice to any other grounds to move to quash or defenses thereto, but it shall be the sole basis for moving to quash on the grounds of a conflict of law related to a qualifying foreign government.

(B) Upon receipt of a motion filed pursuant to subparagraph (A), the court shall afford the governmental entity that applied for or issued the legal process under this section the opportunity to respond. The court may modify or quash the legal process, as appropriate, only if the court finds that-

(i) the required disclosure would cause the provider to violate the laws of a qualifying foreign government;

18 USC 2703 – STORED COMMUNICATIONS ACT

- (ii) based on the totality of the circumstances, the interests of justice dictate that the legal process should be modified or quashed; and
- (iii) the customer or subscriber is not a United States person and does not reside in the United States.

(3) COMITY ANALYSIS.-For purposes of making a determination under paragraph (2)(B)(ii), the court shall take into account, as appropriate-

- (A) the interests of the United States, including the investigative interests of the governmental entity seeking to require the disclosure;
- (B) the interests of the qualifying foreign government in preventing any prohibited disclosure;
- (C) the likelihood, extent, and nature of penalties to the provider or any employees of the provider as a result of inconsistent legal requirements imposed on the provider;
- (D) the location and nationality of the subscriber or customer whose communications are being sought, if known, and the nature and extent of the subscriber or customer's connection to the United States, or if the legal process has been sought on behalf of a foreign authority pursuant to section 3512, the nature and extent of the subscriber or customer's connection to the foreign authority's country;
- (E) the nature and extent of the provider's ties to and presence in the United States;
- (F) the importance to the investigation of the information required to be disclosed;
- (G) the likelihood of timely and effective access to the information required to be disclosed through means that would cause less serious negative consequences; and
- (H) if the legal process has been sought on behalf of a foreign authority pursuant to section 3512, the investigative interests of the foreign authority making the request for assistance.

(4) DISCLOSURE OBLIGATIONS DURING PENDENCY OF CHALLENGE.-A service provider shall preserve, but not be obligated to produce, information sought during the pendency of a motion brought under this subsection, unless the court finds that immediate production is necessary to prevent an adverse result identified in section 2705(a)(2).

(5) DISCLOSURE TO QUALIFYING FOREIGN GOVERNMENT.-

- (A) It shall not constitute a violation of a protective order issued under section 2705 for a provider of electronic communication service to the public or remote computing service to disclose to the entity within a qualifying foreign government, designated in an executive agreement under section 2523, the fact of the existence of legal process issued under this section seeking the contents of a wire or electronic communication

18 USC 2703 – STORED COMMUNICATIONS ACT

of a customer or subscriber who is a national or resident of the qualifying foreign government.

(B) Nothing in this paragraph shall be construed to modify or otherwise affect any other authority to make a motion to modify or quash a protective order issued under section 2705.

18 USC 2709 – STORED COMMUNICATIONS ACT

TITLE 18, SECTION 2709, UNITED STATES CODE
(THE “STORED COMMUNICATIONS ACT”)

COUNTERINTELLIGENCE ACCESS TO TELEPHONE TOLL AND TRANSACTIONAL RECORDS

SECTION 2709.

(a) DUTY TO PROVIDE.-A wire or electronic communication service provider shall comply with a request for subscriber information and toll billing records information, or electronic communication transactional records in its custody or possession made by the Director of the Federal Bureau of Investigation under subsection (b) of this section.

(b) REQUIRED CERTIFICATION.-The Director of the Federal Bureau of Investigation, or his designee in a position not lower than Deputy Assistant Director at Bureau headquarters or a Special Agent in Charge in a Bureau field office designated by the Director, may, using a term that specifically identifies a person, entity, telephone number, or account as the basis for a request-

(1) request the name, address, length of service, and local and long distance toll billing records of a person or entity if the Director (or his designee) certifies in writing to the wire or electronic communication service provider to which the request is made that the name, address, length of service, and toll billing records sought are relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely on the basis of activities protected by the first amendment to the Constitution of the United States; and

(2) request the name, address, and length of service of a person or entity if the Director (or his designee) certifies in writing to the wire or electronic communication service provider to which the request is made that the information sought is relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution of the United States.

(c) PROHIBITION OF CERTAIN DISCLOSURE.-

(1) PROHIBITION.-

(A) IN GENERAL.-If a certification is issued under subparagraph (B) and notice of the right to judicial review under subsection (d) is provided, no wire or electronic communication service provider that receives a request under subsection (b), or officer, employee, or agent thereof, shall disclose to

18 USC 2709 – STORED COMMUNICATIONS ACT

any person that the Federal Bureau of Investigation has sought or obtained access to information or records under this section.

(B) CERTIFICATION.-The requirements of subparagraph (A) shall apply if the Director of the Federal Bureau of Investigation, or a designee of the Director whose rank shall be no lower than Deputy Assistant Director at Bureau headquarters or a Special Agent in Charge of a Bureau field office, certifies that the absence of a prohibition of disclosure under this subsection may result in-

- (i) a danger to the national security of the United States;
- (ii) interference with a criminal, counterterrorism, or counterintelligence investigation;
- (iii) interference with diplomatic relations; or
- (iv) danger to the life or physical safety of any person.

(2) EXCEPTION.-

(A) IN GENERAL.-A wire or electronic communication service provider that receives a request under subsection (b), or officer, employee, or agent thereof, may disclose information otherwise subject to any applicable nondisclosure requirement to-

- (i) those persons to whom disclosure is necessary in order to comply with the request;
- (ii) an attorney in order to obtain legal advice or assistance regarding the request; or
- (iii) other persons as permitted by the Director of the Federal Bureau of Investigation or the designee of the Director.

(B) APPLICATION.-A person to whom disclosure is made under subparagraph (A) shall be subject to the nondisclosure requirements applicable to a person to whom a request is issued under subsection (b) in the same manner as the person to whom the request is issued.

(C) NOTICE.-Any recipient that discloses to a person described in subparagraph (A) information otherwise subject to a nondisclosure requirement shall notify the person of the applicable nondisclosure requirement.

(D) IDENTIFICATION OF DISCLOSURE RECIPIENTS.-At the request of the Director of the Federal Bureau of Investigation or the designee of the Director, any person making or intending to make a disclosure under clause (i) or (iii) of subparagraph (A) shall identify to the Director or such designee the person to whom such disclosure will be made or to whom such disclosure was made prior to the request.

(d) JUDICIAL REVIEW.-

18 USC 2709 – STORED COMMUNICATIONS ACT

(1) IN GENERAL.-A request under subsection (b) or a nondisclosure requirement imposed in connection with such request under subsection (c) shall be subject to judicial review under section 3511.

(2) NOTICE.-A request under subsection (b) shall include notice of the availability of judicial review described in paragraph (1).

(e) DISSEMINATION BY BUREAU.-The Federal Bureau of Investigation may disseminate information and records obtained under this section only as provided in guidelines approved by the Attorney General for foreign intelligence collection and foreign counterintelligence investigations conducted by the Federal Bureau of Investigation, and, with respect to dissemination to an agency of the United States, only if such information is clearly relevant to the authorized responsibilities of such agency.

(f) REQUIREMENT THAT CERTAIN CONGRESSIONAL BODIES BE INFORMED.-On a semiannual basis the Director of the Federal Bureau of Investigation shall fully inform the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate, and the Committee on the Judiciary of the House of Representatives and the Committee on the Judiciary of the Senate, concerning all requests made under subsection (b) of this section.

(g) LIBRARIES.-A library (as that term is defined in section 213(1) of the Library Services and Technology Act (20 U.S.C. 9122(1)), the services of which include access to the Internet, books, journals, magazines, newspapers, or other similar forms of communication in print or digitally by patrons for their use, review, examination, or circulation, is not a wire or electronic communication service provider for purposes of this section, unless the library is providing the services defined in section 2510(15) ("electronic communication service") of this title.

TITLE 12, SECTION 3414, UNITED STATES CODE
(THE “RIGHT TO FINANCIAL PRIVACY ACT”)

SPECIAL PROCEDURES

SECTION 3414.

(a) ACCESS TO FINANCIAL RECORDS FOR CERTAIN INTELLIGENCE AND PROTECTIVE PURPOSES

(1) Nothing in this chapter (except sections 3415, 3417, 3418, and 3421 1 of this title) shall apply to the production and disclosure of financial records pursuant to requests from-

(A) a Government authority authorized to conduct foreign counter- or foreign positive-intelligence activities for purposes of conducting such activities;

(B) the Secret Service for the purpose of conducting its protective functions (18 U.S.C. 3056; 18 U.S.C. 3056A, Public Law 90–331, 1 as amended); or

(C) a Government authority authorized to conduct investigations of, or intelligence or counterintelligence analyses related to, international terrorism for the purpose of conducting such investigations or analyses.

(2) In the instances specified in paragraph (1), the Government authority shall submit to the financial institution the certificate required in section 3403(b) of this title signed by a supervisory official of a rank designated by the head of the Government authority and a term that specifically identifies a customer, entity, or account to be used as the basis for the production and disclosure of financial records.

(3)

(A) If the Government authority described in paragraph (1) or the Secret Service, as the case may be, certifies that otherwise there may result a danger to the national security of the United States, interference with a criminal, counterterrorism, or counterintelligence investigation, interference with diplomatic relations, or danger to the life or physical safety of any person, no financial institution, or officer, employee, or agent of such institution, shall disclose to any person (other than those to whom such disclosure is necessary to comply with the request or an attorney to obtain legal advice or legal assistance with respect to the request) that the Government authority or the Secret Service has sought or obtained access to a customer's financial records.

(B) The request shall notify the person or entity to whom the request is directed of the nondisclosure requirement under subparagraph (A).

12 USC 3414 – RIGHT TO FINANCIAL PRIVACY ACT

(C) Any recipient disclosing to those persons necessary to comply with the request or to an attorney to obtain legal advice or legal assistance with respect to the request shall inform such persons of any applicable nondisclosure requirement. Any person who receives a disclosure under this subsection shall be subject to the same prohibitions on disclosure under subparagraph (A).

(D) At the request of the authorized Government authority or the Secret Service, any person making or intending to make a disclosure under this section shall identify to the requesting official of the authorized Government authority or the Secret Service the person to whom such disclosure will be made or to whom such disclosure was made prior to the request, except that nothing in this section shall require a person to inform the requesting official of the authorized Government authority or the Secret Service of the identity of an attorney to whom disclosure was made or will be made to obtain legal advice or legal assistance with respect to the request for financial records under this subsection.

(4) The Government authority specified in paragraph (1) shall compile an annual tabulation of the occasions in which this section was used.

(5)

(A) Financial institutions, and officers, employees, and agents thereof, shall comply with a request for a customer's or entity's financial records made pursuant to this subsection by the Federal Bureau of Investigation when the Director of the Federal Bureau of Investigation (or the Director's designee in a position not lower than Deputy Assistant Director at Bureau headquarters or a Special Agent in Charge in a Bureau field office designated by the Director) certifies in writing to the financial institution that such records are sought for foreign counter intelligence 2 purposes to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution of the United States.

(B) The Federal Bureau of Investigation may disseminate information obtained pursuant to this paragraph only as provided in guidelines approved by the Attorney General for foreign intelligence collection and foreign counterintelligence investigations conducted by the Federal Bureau of Investigation, and, with respect to dissemination to an agency of the United States, only if such information is clearly relevant to the authorized responsibilities of such agency.

(C) On the dates provided in section 3106 of title 50, the Attorney General shall fully inform the congressional intelligence committees (as defined in

12 USC 3414 – RIGHT TO FINANCIAL PRIVACY ACT

section 3003 of title 50) concerning all requests made pursuant to this paragraph.

(b) EMERGENCY ACCESS TO FINANCIAL RECORDS

(1) Nothing in this chapter shall prohibit a Government authority from obtaining financial records from a financial institution if the Government authority determines that delay in obtaining access to such records would create imminent danger of-

- (A) physical injury to any person;
- (B) serious property damage; or
- (C) flight to avoid prosecution.

(2) In the instances specified in paragraph (1), the Government shall submit to the financial institution the certificate required in section 3403(b) of this title signed by a supervisory official of a rank designated by the head of the Government authority.

(3) Within five days of obtaining access to financial records under this subsection, the Government authority shall file with the appropriate court a signed, sworn statement of a supervisory official of a rank designated by the head of the Government authority setting forth the grounds for the emergency access. The Government authority shall thereafter comply with the notice provisions of section 3409(c) of this title.

(4) The Government authority specified in paragraph (1) shall compile an annual tabulation of the occasions in which this section was used.

(c) PROHIBITION OF CERTAIN DISCLOSURE

(1) PROHIBITION

(A) IN GENERAL

If a certification is issued under subparagraph (B) and notice of the right to judicial review under subsection (d) is provided, no financial institution that receives a request under subsection (a), or officer, employee, or agent thereof, shall disclose to any person that the Federal Bureau of Investigation has sought or obtained access to information or records under subsection (a).

(B) CERTIFICATION

The requirements of subparagraph (A) shall apply if the Director of the Federal Bureau of Investigation, or a designee of the Director whose rank shall be no lower than Deputy Assistant Director at Bureau headquarters or a Special Agent in Charge of a Bureau field office, certifies that the absence of a prohibition of disclosure under this subsection may result in-

- (i) a danger to the national security of the United States;
- (ii) interference with a criminal, counterterrorism, or counterintelligence investigation;

12 USC 3414 – RIGHT TO FINANCIAL PRIVACY ACT

- (iii) interference with diplomatic relations; or
- (iv) danger to the life or physical safety of any person.

(2) EXCEPTION

(A) IN GENERAL

A financial institution that receives a request under subsection (a), or officer, employee, or agent thereof, may disclose information otherwise subject to any applicable nondisclosure requirement to-

- (i) those persons to whom disclosure is necessary in order to comply with the request;
- (ii) an attorney in order to obtain legal advice or assistance regarding the request; or
- (iii) other persons as permitted by the Director of the Federal Bureau of Investigation or the designee of the Director.

(B) APPLICATION

A person to whom disclosure is made under subparagraph (A) shall be subject to the nondisclosure requirements applicable to a person to whom a request is issued under subsection (a) in the same manner as the person to whom the request is issued.

(C) NOTICE

Any recipient that discloses to a person described in subparagraph (A) information otherwise subject to a nondisclosure requirement shall inform the person of the applicable nondisclosure requirement.

(D) IDENTIFICATION OF DISCLOSURE RECIPIENTS

At the request of the Director of the Federal Bureau of Investigation or the designee of the Director, any person making or intending to make a disclosure under clause (i) or (iii) of subparagraph (A) shall identify to the Director or such designee the person to whom such disclosure will be made or to whom such disclosure was made prior to the request.

(d) JUDICIAL REVIEW

(1) IN GENERAL

A request under subsection (a) or a nondisclosure requirement imposed in connection with such request under subsection (c) shall be subject to judicial review under section 3511 of title 18.

(2) NOTICE

A request under subsection (a) shall include notice of the availability of judicial review described in paragraph (1).

(e) DEFINITION OF "FINANCIAL INSTITUTION"

For purposes of this section, and sections 3415 and 3417 of this title insofar as they relate to the operation of this section, the term "financial institution" has the same meaning as in subsections (a)(2) and (c)(1) of section 5312 of title 31, except that, for purposes of this section, such term shall include only such

12 USC 3414 – RIGHT TO FINANCIAL PRIVACY ACT

a financial institution any part of which is located inside any State or territory of the United States, the District of Columbia, Puerto Rico, Guam, American Samoa, the Commonwealth of the Northern Mariana Islands, or the United States Virgin Islands.

TITLE 15, SECTION 1681u, UNITED STATES CODE
(THE “FAIR CREDIT REPORTING ACT”)

DISCLOSURES TO FBI FOR COUNTERINTELLIGENCE PURPOSES

SECTION 1681u.

(a) IDENTITY OF FINANCIAL INSTITUTIONS

Notwithstanding section 1681b of this title or any other provision of this subchapter, a consumer reporting agency shall furnish to the Federal Bureau of Investigation the names and addresses of all financial institutions (as that term is defined in section 3401 of title 12) at which a consumer maintains or has maintained an account, to the extent that information is in the files of the agency, when presented with a written request for that information that includes a term that specifically identifies a consumer or account to be used as the basis for the production of that information, signed by the Director of the Federal Bureau of Investigation, or the Director's designee in a position not lower than Deputy Assistant Director at Bureau headquarters or a Special Agent in Charge of a Bureau field office designated by the Director, which certifies compliance with this section. The Director or the Director's designee may make such a certification only if the Director or the Director's designee has determined in writing, that such information is sought for the conduct of an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution of the United States.

(b) IDENTIFYING INFORMATION

Notwithstanding the provisions of section 1681b of this title or any other provision of this subchapter, a consumer reporting agency shall furnish identifying information respecting a consumer, limited to name, address, former addresses, places of employment, or former places of employment, to the Federal Bureau of Investigation when presented with a written request that includes a term that specifically identifies a consumer or account to be used as the basis for the production of that information, signed by the Director or the Director's designee in a position not lower than Deputy Assistant Director at Bureau headquarters or a Special Agent in Charge of a Bureau field office designated by the Director, which certifies compliance with this subsection. The Director or the Director's designee may make such a certification only if the Director or the Director's designee has determined in writing that such information is sought for the conduct of an authorized investigation to protect against international

15 USC 1681U – FAIR CREDIT REPORTING ACT

terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution of the United States.

(c) COURT ORDER FOR DISCLOSURE OF CONSUMER REPORTS

Notwithstanding section 1681b of this title or any other provision of this subchapter, if requested in writing by the Director of the Federal Bureau of Investigation, or a designee of the Director in a position not lower than Deputy Assistant Director at Bureau headquarters or a Special Agent in Charge in a Bureau field office designated by the Director, a court may issue an order ex parte, which shall include a term that specifically identifies a consumer or account to be used as the basis for the production of the information, directing a consumer reporting agency to furnish a consumer report to the Federal Bureau of Investigation, upon a showing in camera that the consumer report is sought for the conduct of an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution of the United States. The terms of an order issued under this subsection shall not disclose that the order is issued for purposes of a counterintelligence investigation.

(d) PROHIBITION OF CERTAIN DISCLOSURE

(1) PROHIBITION

(A) IN GENERAL

If a certification is issued under subparagraph (B) and notice of the right to judicial review under subsection (e) is provided, no consumer reporting agency that receives a request under subsection (a) or (b) or an order under subsection (c), or officer, employee, or agent thereof, shall disclose or specify in any consumer report, that the Federal Bureau of Investigation has sought or obtained access to information or records under subsection (a), (b), or (c).

(B) CERTIFICATION

The requirements of subparagraph (A) shall apply if the Director of the Federal Bureau of Investigation, or a designee of the Director whose rank shall be no lower than Deputy Assistant Director at Bureau headquarters or a Special Agent in Charge of a Bureau field office, certifies that the absence of a prohibition of disclosure under this subsection may result in-

- (i) a danger to the national security of the United States;
- (ii) interference with a criminal, counterterrorism, or counterintelligence investigation;
- (iii) interference with diplomatic relations; or
- (iv) danger to the life or physical safety of any person.

15 USC 1681U – FAIR CREDIT REPORTING ACT

(2) EXCEPTION

(A) IN GENERAL

A consumer reporting agency that receives a request under subsection (a) or (b) or an order under subsection (c), or officer, employee, or agent thereof, may disclose information otherwise subject to any applicable nondisclosure requirement to-

- (i) those persons to whom disclosure is necessary in order to comply with the request;
- (ii) an attorney in order to obtain legal advice or assistance regarding the request; or
- (iii) other persons as permitted by the Director of the Federal Bureau of Investigation or the designee of the Director.

(B) APPLICATION

A person to whom disclosure is made under subparagraph (A) shall be subject to the nondisclosure requirements applicable to a person to whom a request under subsection (a) or (b) or an order under subsection (c) is issued in the same manner as the person to whom the request is issued.

(C) NOTICE

Any recipient that discloses to a person described in subparagraph (A) information otherwise subject to a nondisclosure requirement shall inform the person of the applicable nondisclosure requirement.

(D) IDENTIFICATION OF DISCLOSURE RECIPIENTS

At the request of the Director of the Federal Bureau of Investigation or the designee of the Director, any person making or intending to make a disclosure under clause (i) or (iii) of subparagraph (A) shall identify to the Director or such designee the person to whom such disclosure will be made or to whom such disclosure was made prior to the request.

(e) JUDICIAL REVIEW

(1) IN GENERAL

A request under subsection (a) or (b) or an order under subsection (c) or a non-disclosure requirement imposed in connection with such request under subsection (d) shall be subject to judicial review under section 3511 of title 18.

(2) NOTICE

A request under subsection (a) or (b) or an order under subsection (c) shall include notice of the availability of judicial review described in paragraph (1).

(f) PAYMENT OF FEES

The Federal Bureau of Investigation shall, subject to the availability of appropriations, pay to the consumer reporting agency assembling or providing report or information in accordance with procedures established under this section a fee for reimbursement for such costs as are reasonably necessary and

15 USC 1681U – FAIR CREDIT REPORTING ACT

which have been directly incurred in searching, reproducing, or transporting books, papers, records, or other data required or requested to be produced under this section.

(g) LIMIT ON DISSEMINATION

The Federal Bureau of Investigation may not disseminate information obtained pursuant to this section outside of the Federal Bureau of Investigation, except to other Federal agencies as may be necessary for the approval or conduct of a foreign counterintelligence investigation, or, where the information concerns a person subject to the Uniform Code of Military Justice, to appropriate investigative authorities within the military department concerned as may be necessary for the conduct of a joint foreign counterintelligence investigation.

(h) RULES OF CONSTRUCTION

Nothing in this section shall be construed to prohibit information from being furnished by the Federal Bureau of Investigation pursuant to a subpoena or court order, in connection with a judicial or administrative proceeding to enforce the provisions of this subchapter. Nothing in this section shall be construed to authorize or permit the withholding of information from the Congress.

(i) REPORTS TO CONGRESS

- (1) On a semiannual basis, the Attorney General shall fully inform the Permanent Select Committee on Intelligence and the Committee on Banking, Finance and Urban Affairs of the House of Representatives, and the Select Committee on Intelligence and the Committee on Banking, Housing, and Urban Affairs of the Senate concerning all requests made pursuant to subsections (a), (b), and (c).
- (2) In the case of the semiannual reports required to be submitted under paragraph (1) to the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate, the submittal dates for such reports shall be as provided in section 3106 of title 50.

(j) DAMAGES

Any agency or department of the United States obtaining or disclosing any consumer reports, records, or information contained therein in violation of this section is liable to the consumer to whom such consumer reports, records, or information relate in an amount equal to the sum of-

- (1) \$100, without regard to the volume of consumer reports, records, or information involved;
- (2) any actual damages sustained by the consumer as a result of the disclosure;
- (3) if the violation is found to have been willful or intentional, such punitive damages as a court may allow; and

15 USC 1681U – FAIR CREDIT REPORTING ACT

(4) in the case of any successful action to enforce liability under this subsection, the costs of the action, together with reasonable attorney fees, as determined by the court.

(k) DISCIPLINARY ACTIONS FOR VIOLATIONS

If a court determines that any agency or department of the United States has violated any provision of this section and the court finds that the circumstances surrounding the violation raise questions of whether or not an officer or employee of the agency or department acted willfully or intentionally with respect to the violation, the agency or department shall promptly initiate a proceeding to determine whether or not disciplinary action is warranted against the officer or employee who was responsible for the violation.

(l) GOOD-FAITH EXCEPTION

Notwithstanding any other provision of this subchapter, any consumer reporting agency or agent or employee thereof making disclosure of consumer reports or identifying information pursuant to this subsection in good-faith reliance upon a certification of the Federal Bureau of Investigation pursuant to provisions of this section shall not be liable to any person for such disclosure under this subchapter, the constitution of any State, or any law or regulation of any State or any political subdivision of any State.

(m) LIMITATION OF REMEDIES

Notwithstanding any other provision of this subchapter, the remedies and sanctions set forth in this section shall be the only judicial remedies and sanctions for violation of this section.

(n) INJUNCTIVE RELIEF

In addition to any other remedy contained in this section, injunctive relief shall be available to require compliance with the procedures of this section. In the event of any successful action under this subsection, costs together with reasonable attorney fees, as determined by the court, may be recovered.

TITLE 28, SECTION 0.85, CODE OF FEDERAL REGULATIONS

GENERAL FUNCTIONS

[OF THE DIRECTOR OF THE FEDERAL BUREAU OF INVESTIGATION]

SECTION 0.85.

The Director of the Federal Bureau of Investigation shall:

(a) Investigate violations of the laws, including the criminal drug laws, of the United States and collect evidence in cases in which the United States is or may be a party in interest, except in cases in which such responsibility is by statute or otherwise exclusively assigned to another investigative agency. The Director's authority to investigate violations of and collect evidence in cases involving the criminal drug laws of the United States is concurrent with such authority of the Administrator of the Drug Enforcement Administration under § 0.100 of this part. In investigating violations of such laws and in collecting evidence in such cases, the Director may exercise so much of the authority vested in the Attorney General by sections 1 and 2 of Reorganization Plan No. 1 of 1968, section 1 of Reorganization Plan No. 2 of 1973 and the Comprehensive Drug Abuse Prevention and Control Act of 1970, as amended, as he determines is necessary. He may also release FBI information on the same terms and for the same purposes that the Administrator of the Drug Enforcement Administration may disclose DEA information under § 0.103 of this part. The Director and his authorized delegates may seize, forfeit and remit or mitigate the forfeiture of property in accordance with 21 U.S.C. 881, 21 CFR 1316.71 through 1316.81, and 28 CFR 9.1 through 9.7.

(b) Conduct the acquisition, collection, exchange, classification and preservation of fingerprints and identification records from criminal justice and other governmental agencies, including fingerprints voluntarily submitted by individuals for personal identification purposes; provide expert testimony in Federal, State and local courts as to fingerprint examinations; and provide fingerprint training and provide identification assistance in disasters and for other humanitarian purposes.

(c) Conduct personnel investigations requisite to the work of the Department of Justice and whenever required by statute or otherwise.

(d) Carry out the Presidential directive of September 6, 1939, as reaffirmed by Presidential directives of January 8, 1943, July 24, 1950, and December 15, 1953, designating the Federal Bureau of Investigation to take charge of investigative work in matters relating to espionage, sabotage, subversive activities, and related matters, including investigating any potential violations of the Arms Export Control Act, the Export Administration Act, the Trading with

28 CFR 0.85 – GENERAL FUNCTIONS OF THE DIRECTOR OF THE FBI

the Enemy Act, or the International Emergency Economic Powers Act, relating to any foreign counterintelligence matter.

(e) Establish and conduct law enforcement training programs to provide training for State and local law enforcement personnel; operate the Federal Bureau of Investigation National Academy; develop new approaches, techniques, systems, equipment, and devices to improve and strengthen law enforcement and assist in conducting State and local training programs, pursuant to section 404 of the Omnibus Crime Control and Safe Streets Act of 1968, 82 Stat. 204.

(f) Operate a central clearinghouse for police statistics under the Uniform Crime Reporting Program, and a computerized nationwide index of law enforcement information under the National Crime Information Center.

(g) Operate the Federal Bureau of Investigation Laboratory to serve not only the Federal Bureau of Investigation, but also to provide, without cost, technical and scientific assistance, including expert testimony in Federal or local courts, for all duly constituted law enforcement agencies, other organizational units of the Department of Justice, and other Federal agencies, which may desire to avail themselves of the service. As provided for in procedures agreed upon between the Secretary of State and the Attorney General, the services of the Federal Bureau of Investigation Laboratory may also be made available to foreign law enforcement agencies and courts.

(h) Make recommendations to the Office of Personnel Management in connection with applications for retirement under 5 U.S.C. 8336(c).

(i) Investigate alleged fraudulent conduct in connection with operations of the Department of Housing and Urban Development and other alleged violations of the criminal provisions of the National Housing Act, including 18 U.S.C. 1010.

(j) Exercise the power and authority vested in the Attorney General to approve and conduct the exchanges of identification records enumerated at § 50.12(a) of this chapter.

(k) Payment of awards (including those over \$10,000) under 28 U.S.C. 524(c)(2), and purchase of evidence (including the authority to pay more than \$100,000) under 28 U.S.C. 524(c)(1)(F).

(l) Exercise Lead Agency responsibility in investigating all crimes for which it has primary or concurrent jurisdiction and which involve terrorist activities or acts in preparation of terrorist activities within the statutory jurisdiction of the United States. Within the United States, this would include the collection, coordination, analysis, management and dissemination of intelligence and criminal information as appropriate. If another Federal agency identifies an individual who is engaged in terrorist activities or in acts in preparation of terrorist activities, that agency is requested to promptly notify the FBI. Terrorism includes the unlawful use of force and violence against persons or property to

28 CFR 0.85 – GENERAL FUNCTIONS OF THE DIRECTOR OF THE FBI

intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives.

(m) Carry out the Department's responsibilities under the Hate Crime Statistics Act.

(n) Exercise the authority vested in the Attorney General under section 528(a), Public Law 101-509, to accept from federal departments and agencies the services of law enforcement personnel to assist the Department of Justice in the investigation and prosecution of fraud or other criminal or unlawful activity in or against any federally insured financial institution or the Resolution Trust Corporation, and to coordinate the activities of such law enforcement personnel in the conduct of such investigations and prosecutions.

(o) Carry out the responsibilities conferred upon the Attorney General under the Communications Assistance for Law Enforcement Act, Title I of Pub. L. 103-414 (108 Stat. 4279), subject to the general supervision and direction of the Attorney General.

[Order No. 423-69, 34 FR 20388, Dec. 31, 1969]

TITLE 10, SECTION 431, UNITED STATES CODE

AUTHORITY TO ENGAGE IN COMMERCIAL ACTIVITIES AS SECURITY FOR INTELLIGENCE COLLECTION ACTIVITIES

SECTION 431.

- (a) **AUTHORITY.**-The Secretary of Defense, subject to the provisions of this subchapter, may authorize the conduct of those commercial activities necessary to provide security for authorized intelligence collection activities abroad undertaken by the Department of Defense. No commercial activity may be initiated pursuant to this subchapter after December 31, 2024.
- (b) **INTERAGENCY COORDINATION AND SUPPORT.**-Any such activity shall-
- (1) be coordinated with, and (where appropriate) be supported by, the Director of the Central Intelligence Agency; and
 - (2) to the extent the activity takes place within the United States, be coordinated with, and (where appropriate) be supported by, the Director of the Federal Bureau of Investigation.
- (c) **DEFINITIONS.**-In this subchapter:
- (1) The term "commercial activities" means activities that are conducted in a manner consistent with prevailing commercial practices and includes-
 - (A) the acquisition, use, sale, storage and disposal of goods and services;
 - (B) entering into employment contracts and leases and other agreements for real and personal property;
 - (C) depositing funds into and withdrawing funds from domestic and foreign commercial business or financial institutions;
 - (D) acquiring licenses, registrations, permits, and insurance; and
 - (E) establishing corporations, partnerships, and other legal entities.
 - (2) The term "intelligence collection activities" means the collection of foreign intelligence and counterintelligence information.

TITLE 18, SECTION 1030, UNITED STATES CODE

FRAUD AND RELATED ACTIVITY IN CONNECTION WITH COMPUTERS

SECTION 1030.

(a) Whoever-

(1) having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph y. of section 11 of the Atomic Energy Act of 1954, with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it;

(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains-

(A) information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);

(B) information from any department or agency of the United States; or

(C) information from any protected computer;

(3) intentionally, without authorization to access any nonpublic computer of a department or agency of the United States, accesses such a computer of that department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the United States and such conduct affects that use by or for the Government of the United States;

(4) knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than \$5,000 in any 1-year period;

(5)

10 USC 431 – COMMERCIAL ACTIVITIES

(A) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;

(B) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or

(C) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage and loss.

(6) knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information through which a computer may be accessed without authorization, if-

(A) such trafficking affects interstate or foreign commerce; or

(B) such computer is used by or for the Government of the United States;

(7) with intent to extort from any person any money or other thing of value, transmits in interstate or foreign commerce any communication containing any-

(A) threat to cause damage to a protected computer;

(B) threat to obtain information from a protected computer without authorization or in excess of authorization or to impair the confidentiality of information obtained from a protected computer without authorization or by exceeding authorized access; or

(C) demand or request for money or other thing of value in relation to damage to a protected computer, where such damage was caused to facilitate the extortion;

shall be punished as provided in subsection (c) of this section.

(b) Whoever conspires to commit or attempts to commit an offense under subsection (a) of this section shall be punished as provided in subsection (c) of this section.

(c) The punishment for an offense under subsection (a) or (b) of this section is-

(1)

(A) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(1) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and

(B) a fine under this title or imprisonment for not more than twenty years, or both, in the case of an offense under subsection (a)(1) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

(2)

(A) except as provided in subparagraph (B), a fine under this title or imprisonment for not more than one year, or both, in the case of an offense under subsection (a)(2), (a)(3), or (a)(6) of this section which does not occur

10 USC 431 – COMMERCIAL ACTIVITIES

after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

(B) a fine under this title or imprisonment for not more than 5 years, or both, in the case of an offense under subsection (a)(2), or an attempt to commit an offense punishable under this subparagraph, if-

(i) the offense was committed for purposes of commercial advantage or private financial gain;

(ii) the offense was committed in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or of any State; or

(iii) the value of the information obtained exceeds \$5,000; and

(C) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(2), (a)(3) or (a)(6) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

(3)

(A) a fine under this title or imprisonment for not more than five years, or both, in the case of an offense under subsection (a)(4) or (a)(7) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and

(B) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(4), or (a)(7) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

(4)

(A) except as provided in subparagraphs (E) and (F), a fine under this title, imprisonment for not more than 5 years, or both, in the case of-

(i) an offense under subsection (a)(5)(B), which does not occur after a conviction for another offense under this section, if the offense caused (or, in the case of an attempted offense, would, if completed, have caused)-

(I) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least \$5,000 in value;

10 USC 431 – COMMERCIAL ACTIVITIES

- (II) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals;
 - (III) physical injury to any person;
 - (IV) a threat to public health or safety;
 - (V) damage affecting a computer used by or for an entity of the United States Government in furtherance of the administration of justice, national defense, or national security; or
 - (VI) damage affecting 10 or more protected computers during any 1-year period; or
- (ii) an attempt to commit an offense punishable under this subparagraph;
- (B) except as provided in subparagraphs (E) and (F), a fine under this title, imprisonment for not more than 10 years, or both, in the case of-
- (i) an offense under subsection (a)(5)(A), which does not occur after a conviction for another offense under this section, if the offense caused (or, in the case of an attempted offense, would, if completed, have caused) a harm provided in subclauses (I) through (VI) of subparagraph (A)(i); or
 - (ii) an attempt to commit an offense punishable under this subparagraph;
- (C) except as provided in subparagraphs (E) and (F), a fine under this title, imprisonment for not more than 20 years, or both, in the case of-
- (i) an offense or an attempt to commit an offense under subparagraphs (A) or (B) of subsection (a)(5) that occurs after a conviction for another offense under this section; or
 - (ii) an attempt to commit an offense punishable under this subparagraph;
- (D) a fine under this title, imprisonment for not more than 10 years, or both, in the case of-
- (i) an offense or an attempt to commit an offense under subsection (a)(5)(C) that occurs after a conviction for another offense under this section; or
 - (ii) an attempt to commit an offense punishable under this subparagraph;
- (E) if the offender attempts to cause or knowingly or recklessly causes serious bodily injury from conduct in violation of subsection (a)(5)(A), a fine under this title, imprisonment for not more than 20 years, or both;
- (F) if the offender attempts to cause or knowingly or recklessly causes death from conduct in violation of subsection (a)(5)(A), a fine under this title, imprisonment for any term of years or for life, or both; or
- (G) a fine under this title, imprisonment for not more than 1 year, or both, for-
- (i) any other offense under subsection (a)(5); or
 - (ii) an attempt to commit an offense punishable under this subparagraph.

10 USC 431 – COMMERCIAL ACTIVITIES

(d)

(1) The United States Secret Service shall, in addition to any other agency having such authority, have the authority to investigate offenses under this section.

(2) The Federal Bureau of Investigation shall have primary authority to investigate offenses under subsection (a)(1) for any cases involving espionage, foreign counterintelligence, information protected against unauthorized disclosure for reasons of national defense or foreign relations, or Restricted Data (as that term is defined in section 11y of the Atomic Energy Act of 1954 (42 U.S.C. 2014(y)), except for offenses affecting the duties of the United States Secret Service pursuant to section 3056(a) of this title.

(3) Such authority shall be exercised in accordance with an agreement which shall be entered into by the Secretary of the Treasury and the Attorney General.

(e) As used in this section-

(1) the term "computer" means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device;

(2) the term "protected computer" means a computer-

(A) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government;

(B) which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States; or

(C) that-

(i) is part of a voting system; and

(ii)

(I) is used for the management, support, or administration of a Federal election; or

(II) has moved in or otherwise affects interstate or foreign commerce;

(3) the term "State" includes the District of Columbia, the Commonwealth of Puerto Rico, and any other commonwealth, possession or territory of the United States;

(4) the term "financial institution" means-

10 USC 431 – COMMERCIAL ACTIVITIES

- (A) an institution, with deposits insured by the Federal Deposit Insurance Corporation;
 - (B) the Federal Reserve or a member of the Federal Reserve including any Federal Reserve Bank;
 - (C) a credit union with accounts insured by the National Credit Union Administration;
 - (D) a member of the Federal home loan bank system and any home loan bank;
 - (E) any institution of the Farm Credit System under the Farm Credit Act of 1971;
 - (F) a broker-dealer registered with the Securities and Exchange Commission pursuant to section 15 of the Securities Exchange Act of 1934;
 - (G) the Securities Investor Protection Corporation;
 - (H) a branch or agency of a foreign bank (as such terms are defined in paragraphs (1) and (3) of section 1(b) of the International Banking Act of 1978); and
 - (I) an organization operating under section 25 or section 25(a) of the Federal Reserve Act;
- (5) the term "financial record" means information derived from any record held by a financial institution pertaining to a customer's relationship with the financial institution;
- (6) the term "exceeds authorized access" means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter;
- (7) the term "department of the United States" means the legislative or judicial branch of the Government or one of the executive departments enumerated in section 101 of title 5;
- (8) the term "damage" means any impairment to the integrity or availability of data, a program, a system, or information;
- (9) the term "government entity" includes the Government of the United States, any State or political subdivision of the United States, any foreign country, and any state, province, municipality, or other political subdivision of a foreign country;
- (10) the term "conviction" shall include a conviction under the law of any State for a crime punishable by imprisonment for more than 1 year, an element of which is unauthorized access, or exceeding authorized access, to a computer;
- (11) the term "loss" means any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the

10 USC 431 – COMMERCIAL ACTIVITIES

offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service;

(12) the term "person" means any individual, firm, corporation, educational institution, financial institution, governmental entity, or legal or other entity;

(13) the term "Federal election" means any election (as defined in section 301(1) of the Federal Election Campaign Act of 1971 (52 U.S.C. 30101(1))) for Federal office (as defined in section 301(3) of the Federal Election Campaign Act of 1971 (52 U.S.C. 30101(3))); and

(14) the term "voting system" has the meaning given the term in section 301(b) of the Help America Vote Act of 2002 (52 U.S.C. 21081(b)).

(f) This section does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State, or of an intelligence agency of the United States.

(g) Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief. A civil action for a violation of this section may be brought only if the conduct involves 1 of the factors set forth in subclauses ⁵ (I), (II), (III), (IV), or (V) of subsection (c)(4)(A)(i). Damages for a violation involving only conduct described in subsection (c)(4)(A)(i)(I) are limited to economic damages. No action may be brought under this subsection unless such action is begun within 2 years of the date of the act complained of or the date of the discovery of the damage. No action may be brought under this subsection for the negligent design or manufacture of computer hardware, computer software, or firmware.

(h) The Attorney General and the Secretary of the Treasury shall report to the Congress annually, during the first 3 years following the date of the enactment of this subsection, concerning investigations and prosecutions under subsection (a)(5).

(i)

(1) The court, in imposing sentence on any person convicted of a violation of this section, or convicted of conspiracy to violate this section, shall order, in addition to any other sentence imposed and irrespective of any provision of State law, that such person forfeit to the United States-

(A) such person's interest in any personal property that was used or intended to be used to commit or to facilitate the commission of such violation; and

(B) any property, real or personal, constituting or derived from, any proceeds that such person obtained, directly or indirectly, as a result of such violation.

10 USC 431 – COMMERCIAL ACTIVITIES

(2) The criminal forfeiture of property under this subsection, any seizure and disposition thereof, and any judicial proceeding in relation thereto, shall be governed by the provisions of section 413 of the Comprehensive Drug Abuse Prevention and Control Act of 1970 (21 U.S.C. 853), except subsection (d) of that section.

(j) For purposes of subsection (i), the following shall be subject to forfeiture to the United States and no property right shall exist in them:

(1) Any personal property used or intended to be used to commit or to facilitate the commission of any violation of this section, or a conspiracy to violate this section.

(2) Any property, real or personal, which constitutes or is derived from proceeds traceable to any violation of this section, or a conspiracy to violate this section

TITLE 28, SECTION 533, UNITED STATES CODE

INVESTIGATIVE AND OTHER OFFICIALS; APPOINTMENT

SECTION 533.

The Attorney General may appoint officials-

- (1) to detect and prosecute crimes against the United States;
- (2) to assist in the protection of the person of the President; and
- (3) to assist in the protection of the person of the Attorney General.
- (4) to conduct such other investigations regarding official matters under the control of the Department of Justice and the Department of State as may be directed by the Attorney General.

This section does not limit the authority of departments and agencies to investigate crimes against the United States when investigative jurisdiction has been assigned by law to such departments and agencies.

Statutory Notes and Related Subsidiaries

**FBI Investigations of Espionage by Persons Employed by or Assigned to
United States Diplomatic Missions Abroad**

Pub. L. 101-193, title VI, §603, Nov. 30, 1989, 103 Stat. 1710 , provided that: "Subject to the authority of the Attorney General, the FBI shall supervise the conduct of all investigations of violations of the espionage laws of the United States by persons employed by or assigned to United States diplomatic missions abroad. All departments and agencies shall report immediately to the FBI any information concerning such a violation. All departments and agencies shall provide appropriate assistance to the FBI in the conduct of such investigations. Nothing in this provision shall be construed as establishing a defense to any criminal, civil, or administrative action."