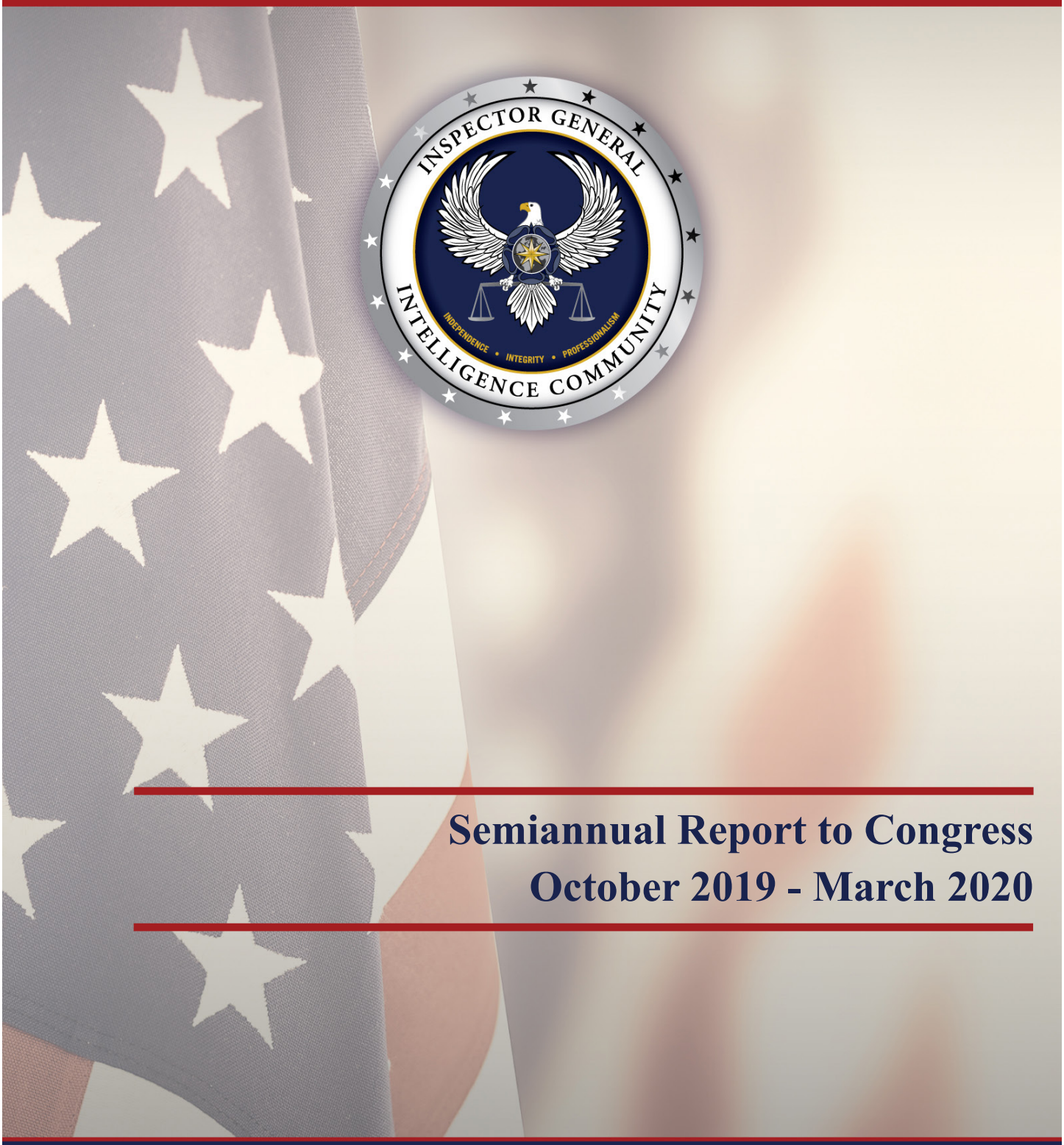
Office of the Inspector General of the Intelligence Community



Semiannual Report to Congress
October 2019 - March 2020

TABLE OF CONTENTS

MESSAGE FROM THE ACTING INSPECTOR GENERAL OF THE INTELLIGENCE COMMUNITY

On behalf of the Office of the Inspector General of the Intelligence Community (IC IG), I am pleased to present our *Semiannual Report* summarizing the team's work and accomplishments for the period of October 1, 2019, through March 31, 2020. I thank everyone whose professionalism, dedication, and support enabled this important work.

I feel privileged to have been appointed as the Acting Inspector General on April 3, 2020. As I have done throughout my 30 years of public service, I take very seriously my Constitutional oath to well and faithfully discharge my duties, and I will continue to uphold the rule of law. I also take very seriously my responsibilities to the people I am entrusted to lead.

The IC IG team remains committed to accomplishing our vital mission to promote economy, efficiency, and effectiveness in the programs and activities within the responsibility of the Director of National Intelligence, and to prevent and detect fraud and abuse in those programs and activities. We are conducting investigations, inspections, audits, and reviews, and also maintaining an effective whistleblower program.

We are working closely and collaboratively with the Intelligence Community Inspectors General Forum, the Council of the Inspectors General on Integrity and Efficiency, the Office of the Director of National Intelligence (ODNI), Congress, and others.

We are guided by the IC IG core values of Integrity, Independence, Commitment, Diversity, and Transparency, and the ODNI core values of Excellence, Courage, Respect, and Integrity.

Like many others around the country and world, the IC IG team continues to be impacted by the ongoing pandemic. We are protecting the health and safety of our people and accomplishing our mission as soon as we reasonably and responsibly can do so. Unfortunately, some of our work (like this *Semiannual Report*) was delayed and some previously-planned projects (highlighted in the *Fiscal Year 2020 Annual Work Plan*) has been postponed.

We appreciate the understanding and support from the Director of National Intelligence, Congress, and others as we continue to navigate through these unprecedented and challenging times together.

The IC IG team is resilient and will continue providing independent and effective oversight to the best of our abilities. As a result, we help improve the Intelligence Community and strengthen the Nation.

Thomas A. Monheim
Acting Inspector General
of the Intelligence Community
July 31, 2020

INTRODUCTION

Authority

The *Intelligence Authorization Act for Fiscal Year 2010* established the Office of the Inspector General of the Intelligence Community (IC IG) within the Office of the Director of National Intelligence (ODNI). The IC IG has the authority to initiate and conduct independent audits, inspections, investigations, and reviews of programs and activities within the responsibility and authority of the Director of National Intelligence (DNI).

IC IG Mission

The IC IG's mission is to provide independent and objective oversight of the programs and activities within the responsibility and authority of the Director of National Intelligence, and to lead and coordinate the efforts of the Intelligence Community Inspectors General Forum.

IC IG Strategic Goal

The IC IG's strategic goal is to have a positive and enduring impact throughout the Intelligence Community, to lead and coordinate the efforts of an integrated Intelligence Community Inspectors General Forum, and to enhance the ability of the United States Intelligence Community to meet national security needs while respecting our nation's laws and reflecting its values.

IC IG Core Values

INTEGRITY

INDEPENDENCE

COMMITMENT

DIVERSITY

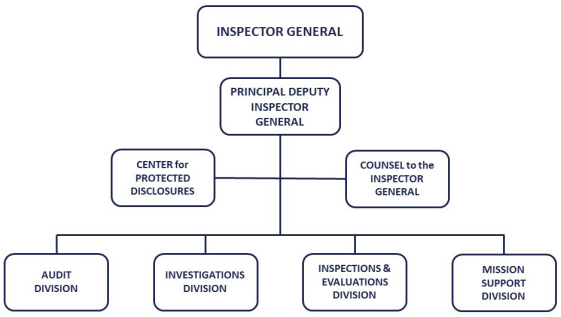
TRANSPARENCY

Independence

The Inspector General of the Intelligence Community is nominated by the President of the United States and confirmed by, and with the advice and consent of, the United States Senate. The Office of the Inspector General of the Intelligence Community bases its findings and conclusions on independent and objective analysis of the facts and evidence that are revealed through audits, investigations, inspections, and programmatic reviews. During this reporting period, the IC IG had full and direct access to all relevant information needed to perform its duties.

Organization

The IC IG's senior management team includes the Inspector General, Principal Deputy Inspector General, Counsel to the IG, five Assistant Inspectors General, and one Center Director.



The IC IG employs a highly skilled, committed, and diverse workforce, including permanent employees (cadre), employees from other Intelligence Community (IC) elements and other government entities on detail to the IC IG (detailees), and contractors. Additional personnel details are listed in the classified Annex of the IC IG's *Semiannual Report* to Congress.

AUDIT DIVISION

The Audit Division conducts independent and objective audits and reviews of ODNI programs and activities, including those non-discretionary audits required by law, such as the annual independent evaluation of ODNI's information security program and practices required by the *Federal Information Security Modernization Act* (FISMA); the annual review of ODNI's compliance with the *Improper Payments Elimination and Recovery Act* (IPERA); the annual risk assessment of purchase and travel card programs; and the biennial report to Congress – prepared jointly with the Departments of Commerce, Defense, Energy, Homeland Security, Justice, and Treasury – on the actions taken to carry out the *Cybersecurity Act of 2015.* The Audit Division participates with other federal agencies and departments in conducting joint reviews of IC programs and activities.

Audit Division activities improve business practices to better support the Intelligence Community's mission; help reduce fraud, waste, abuse, and mismanagement; and promote the economy, efficiency, and effectiveness of programs and operations throughout ODNI and the IC. Audit work focuses on information technology and security, acquisition policies and practices, project management, business practices, human capital, and financial management. Auditors assess whether programs are achieving intended results and whether organizations are complying with laws, regulations, and internal policies.

During the reporting period, the Audit Division led several collaboration and outreach efforts in areas of mutual interest across the IC Audit community. The Audit Division coordinated with Office of the Inspector General (OIG) officers from the Departments of Commerce, Defense, Energy, Homeland Security, Justice, and Treasury on the input to and the issuance of the joint report, *Implementation of the Cybersecurity Information Sharing Act of 2015 (CISA) – Section 107(b).* CISA requires the inspectors general to jointly report to Congress on the actions taken over the most recent two-year period to carry out the statute. In addition, the Audit Division coordinated discussions among OIG officers from the National Reconnaissance Office (NRO), National Security Agency (NSA), National Geospatial-Intelligence Agency (NGA), Defense Intelligence Agency (DIA), and the Central Intelligence Agency (CIA) on the approach for a cross-Community review of information security continuous monitoring (ISCM). Continuous monitoring is a risk management approach to cybersecurity that maintains an accurate picture of an agency's security risk posture; provides visibility into assets; and leverages use of automated data feeds to quantify risk, ensure effectiveness of security controls, and implement prioritized remedies. Answering agreed-upon questions, each OIG will assess their element's implementation of an ISCM program; the IC IG will prepare a capstone report to provide a Community perspective on issues with or lessons learned from implementing continuous monitoring. In other collaboration efforts, an IC IG auditor was assigned to participate on the joint team conducting the external peer review of

NRO OIG's system of quality control; another IC IG auditor was assigned to participate on the joint team conducting the external peer review of CIA OIG's system of quality control.

The IC IG's audit activities are conducted in accordance with generally accepted government auditing standards.

INVESTIGATIONS DIVISION

The Investigations Division is authorized to conduct proactive and reactive criminal and administrative investigations arising from 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. As part of its work, the Investigations Division identifies and reports internal control weaknesses that could render ODNI or other IC programs and systems vulnerable to exploitation, and which could potentially be leveraged for illicit activity resulting in ill-gotten gains. The Investigations Division also plays a pivotal role in tracking and monitoring unauthorized disclosures, and has the discretionary authority to lead independent administrative investigations of selected cases should the Department of Justice decline prosecution. The Division exercises its authority to investigate unauthorized disclosures in consultation with the IG(s) of the involved IC element(s).

The Investigations Division has unique authority to investigate programs and activities across the IC within the responsibility and authority of the DNI. With this authority and responsibility, the Investigations Division coordinates and assists with the prosecution of criminal matters arising from the six independent intelligence agencies: NRO, NGA, NSA, DIA, CIA, and the ODNI.

The IC IG's investigation activities conform to the Council of the Inspectors General on Integrity and Efficiency (CIGIE) standards.

Investigative Activity Overview

The Investigations Division continues to investigate, among other things, cross-Intelligence Community fraud, public corruption, and counterintelligence matters. During this reporting period, the Investigations Division worked on five joint criminal investigations involving ten other law enforcement organizations, including the Federal Bureau of Investigation (FBI), Intelligence Community Offices of Inspectors General, Defense Criminal Investigative Service, and other local and federal investigative agencies, as well as the Department of Justice Public Integrity Section, and the U.S. Attorney's Office for the Eastern District of Virginia. The Investigations Division expects most of these investigations to continue into the next reporting period due to the size, scope, and nature of the matters.

The Investigations Division currently has 28 ongoing investigations (*see* Table 1 below) and published 4 investigative reports this reporting period.

Summaries of Published Investigative Reports

Contractor Cost Mischarging

We did not substantiate allegations that an ODNI contractor employee personally, or through the vendor, simultaneously billed on two different contracts. In addition, the investigation and analysis did not produce any evidence indicating the employee or their respective companies received any preferential treatment from government personnel.

Misuse of Government Resources

We substantiated allegations of misuse of government resources by an ODNI contractor employee. The investigation determined the contractor employee misused government computers for purposes of deception. Specifically, the contractor employee created three fake personas to inappropriately communicate with an unwitting individual by sending over 150 explicit emails.

The investigation also determined the contractor employee's personal use of his Government computer resulted in a loss to the Government of at least $31,914.22, an amount billed to the Government by the vendor without any services provided. As a result, management took action related to two of the suggested recommendations. However, the recommendation to recoup money owed to the Government is still pending.

Contract Mischarging

We did not substantiate allegations of contractor mischarging against an ODNI contractor. Specifically, it was alleged that a sub-contracting company encouraged its employees to work and bill extra hours to the Government contract because it was allegedly slightly behind in projected revenue. Our investigation did not produce any evidence to suggest the sub-contracting company engaged in cost mischarging. We found no evidence that any employee billed or worked extra hours that was not allowed per the contract.

Time and Attendance Fraud

We did not substantiate allegations that an ODNI employee engaged in time and attendance fraud or made false official statements and false claims.

Table 1: Ongoing Investigations

Number of Cases	Case Subject/Allegation
1	Qui Tam – Contract and Procurement Fraud
1	Unauthorized Disclosure
4	Conflict of Interest
6	Contract Cost Mischarging (Labor)
4	Misuse of Government Property (Computer)
3	Abuse of Authority/Retaliation
1	Employee Misconduct
1	Use of Illegal Drugs
1	Mismanagement of Government Resources
1	Waste of Government Resources
1	Misappropriation of Funds
1	Time and Attendance Fraud
1	Theft of Government Funds
1	Wire Fraud
1	Contractor Misconduct
28	**Total Open Investigations**

The IC IG did not issue any subpoenas during this reporting period.

INSPECTIONS AND EVALUATIONS DIVISION

The Inspections and Evaluations Division mission is to conduct oversight activities of programs within the DNI's responsibility and authority. The Inspections and Evaluations Division provides the IC IG with an alternative mechanism to traditional audit and investigative disciplines to assess ODNI and IC programs and activities. The CIGIE Quality Standards for inspections and evaluations gives the Division flexibility to develop tailored approaches for determining efficiency, effectiveness, impact, and/or sustainability of agency operations, programs, or policies. In addition, the Inspections and Evaluations Division also adds a unique benefit to the IC IG by offering a capability to conduct expedited management and program evaluations, and respond to priority issues of concern to the ODNI, the IC, Congress, and the public.

The Inspections and Evaluations Division conducts systematic and independent inspections and evaluations of ODNI components, IC elements, and issue factual evidence-based findings that are timely, credible, and useful for managers, policymakers, and stakeholders. Conclusions drawn from the results of inspections and evaluations generate recommendations for decision makers to streamline operations, reduce unnecessary regulations, improve customer service, and minimize inefficient and ineffective procedures. They also improve the performance

and integration of the ODNI and the broader IC. Using a multidisciplinary staff and various methods for gathering and analyzing data, inspections and evaluations typically analyze information; measure performance; determine compliance with applicable law, regulation, and/or policy; identify savings and funds put to better use; share best practices or promising approaches; and assess allegations of fraud, waste, abuse, and mismanagement. In addition, inspections and evaluations can identify where administrative action is necessary.

During the reporting period, the Inspections and Evaluations Division completed project work across the IC IG's five programmatic objectives. This included improving the efficiency and effectiveness of IC Major Systems Acquisition Cybersecurity Risks; enhancing workforce management by evaluating the IC's security clearance reciprocity practices and assessing ODNI's Senior Executive Service reporting; championing protected disclosures by evaluating implementation of Intelligence Community Directive 701, *Unauthorized Disclosure of Classified Information*; improving oversight by advancing Artificial Intelligence (AI) capability; and integrating the IC by evaluating the IC's foreign language program.

MISSION SUPPORT DIVISION

During this reporting period, IC IG evaluated operations to identify opportunities to enhance efficiencies for more effective delivery of products and services and to better leverage resources for the benefit of the community and expand community collaboration and engagement through such means as cross-community training, recruitment, professional development, and concerted approaches to information technology solutions. As a result, the IC IG's mission support function, formerly named the Management and Administration Division, was restructured to enhance performance, simplify lines of authority, and more rapidly respond to operational needs. We renamed the Division the Mission Support Division (MSD), with responsibilities split between two business areas: (1) Planning and Operations, and (2) Talent Strategy, Workforce Engagement, and Communications.

As a whole, the Mission Support Division provides management and administrative support to the IC IG operational divisions. The Mission Support Division is composed of multidiscipline officers who provide expertise in financial management, human capital and talent management, facilities and logistics management, continuity of operations, administration, classification, *Freedom of Information Act* (FOIA) requests, information technology, communications, and quality assurance. The Division also delivers executive support to the Intelligence Community Inspectors General Forum and its associated committees.

The Planning and Operations Unit supports operational matters across a range of functions, including strategy development, strategy performance oversight, internal management and alignment of resources to IC IG goals and priorities, resource allocation, implementation of cross-cutting business processes, management of support to the statutory Intelligence Community Inspectors General Forum, budget, manpower, contracts, security, information technology, facilities, logistics, quality assurance, information management, classification, FOIA operations, and continuity of operations/emergency preparedness.

The Talent Strategy, Workforce Engagement, and Communications Unit supports human capital and communications activities, including shaping and executing the office's human capital strategy, initiatives, and tactical plan, as well as all IC IG outreach activities, such as media engagements, strategic communications, corporate identity and brand management, and visual communication.

Notable Mission Support achievements during this reporting period include:

- Establishing a plan, systems, and protocols to navigate the office through the COVID-19 pandemic period while protecting the health and safety of the IC IG workforce, and incrementally increasing work capacity to accomplish the IC IG mission reasonably and responsibly.
- In coordination with IC IG senior leadership and collaboration with mission partners, developing and publishing the IC IG *Annual*

Work Plan, a summary of the congressionally directed mandatory and discretionary projects the office will undertake in Fiscal Year 2020 to further the IC IG's statutory responsibility to promote economy, efficiency, and effectiveness in the administration and implementation of the programs and activities within the responsibility and authority of the Director of National Intelligence, and to prevent and detect fraud and abuse in such programs and activities.

- Overseeing the production of statutorily required reports to include the *Semiannual Report*, and conducting strategic analysis to develop the *Capstone Report on the Intelligence Community's Top Management and Performance Challenges for Fiscal Year 2019.*
- Liaising with foreign partners in support of the Inspector General of the Intelligence Community's partnership with the Five Eyes Intelligence Oversight and Review Council.
- Participating in monthly meetings hosted by the Council of the Inspectors General on Integrity and Efficiency and briefing IC IG leadership and personnel on pertinent discussions.

The Mission Support Division is responsible for planning and executing the annual Intelligence Community Inspectors General Conference and Awards Program. This year's program, scheduled to take place in April, was cancelled in mid-March due to concerns over the spread of COVID-19. Building on the strong momentum of the 2019 conference that brought together more than 500 professionals from the Inspector General community, this year's event was to focus on important topics such as artificial intelligence, whistleblowing rights and protections, and emerging national security threats. The recipients of the Intelligence Community Inspectors General National Intelligence Professional Awards will be recognized for their superior performance and exceptional accomplishments at a later date.

During this reporting period, ODNI provided the IC IG adequate funding to fulfill its mission. The budget covered personnel services and general support, including travel, training, equipment, supplies, information technology support, and office automation requirements.

COUNSEL TO THE INSPECTOR GENERAL

The Office of the Counsel to the IC IG ensures that the IC IG team receives independent and confidential legal advice and policy counsel that is without any conflicts of interest in fact or appearance.

The IC IG's main office is in Reston, Virginia.

The Counsel team supports the Investigations Division throughout the investigative process by highlighting and providing guidance on potential legal issues meriting additional or redirected investigative efforts. Counsel supports the Audit Division and the Inspections and Evaluations Division by identifying and interpreting key policy, contract, and legal provisions relevant to reported observations, findings, and recommendations. The Counsel's office assists the Center for Protected Disclosures in evaluating whistleblower disclosures and External Review Panel requests. Attorneys from the Counsel's office also participate in the Intelligence Community Inspectors General Forum, the Forum's Counsels Committee, the IC IG Data Analytics working group, and the Five Eyes Intelligence Oversight and Review Council working groups. The Counsel's office

also provides legal and policy guidance, and reviews matters related to IC IG personnel, administration, training, ethics, independence, and budgetary functions.

The Counsel team also serves as the IC IG's Congressional Liaison. During the reporting period, Counsel arranged for and participated in several congressional briefings with the Inspector General and senior IC IG leadership, including briefings to Members of Congress and bipartisan staff; responded to formal congressional requests for information; and reported on audits in response to congressional interest and legislative mandates. Engagements during this reporting period included the following:

- Appearing before members of the United States Senate Select Committee on Intelligence (SSCI) and the United States House Permanent Select Committee on Intelligence (HPSCI), to discuss matters related to a disclosure submitted to the IC IG of an alleged "urgent concern" pursuant to 50 U.S.C. § 3033(k)(5)(A);
- Engaging with bipartisan SSCI and HPSCI Members and staff to timely respond to inquiries related to ongoing matters within the IC IG;
- Providing comments for and cooperating with Government Accountability Office (GAO) in its review of whistleblower protections in the Intelligence Community; and
- Responding to dozens of letters, emails, and phone calls from the intelligence oversight committees, and other Members and congressional staff to address questions regarding pending legislation and other matters within the IC IG's jurisdiction.

THE CENTER FOR PROTECTED DISCLOSURES

The IC IG's Center for Protected Disclosures (The Center) processes disclosures and complaints reported by whistleblowers and provides guidance to individuals about the options and protections afforded to individuals who may wish to make a protected disclosure to the IC IG and/or Congress, or who believe they have suffered reprisal because they made a protected disclosure. The Center administers requests by employees and contractors in the Intelligence Community for the IC IG to review their allegations of reprisal under Presidential Policy Directive 19 (PPD-19), *Protecting Whistleblowers with Access to Classified Information*, and under section 1104 of the *National Security Act of 1947* (50 U.S.C. 3234) and section 3001(j)(1) of the *Intelligence Reform and Terrorism Prevention Act of 2004* (50 U.S.C. 3341(j)).

The Center includes the IC IG's Hotline Program, which processes allegations of fraud, waste, and abuse of programs and activities within the responsibility and authority of the Director of National Intelligence. The IC IG's Hotline also receives allegations of "Urgent Concerns," and Request for an External Review Panel (ERP).

The Center also processes complaints or information with respect to alleged urgent concerns in accordance with the *Intelligence Community Whistleblower Protection Act* (ICWPA) and the IC IG's authorizing statute, 50 U.S.C. 3033 § (k)(5)(A). In order to file an urgent concern, the law requires that a complainant be "[a]n 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." *Id.* at § 3033(k)(5)(A).

The law also requires that a complainant provide a complaint or information with respect to an "urgent concern," which is defined, in relevant part, as:

> A serious or flagrant problem, abuse, violation of the law or Executive order, or deficiency relating to the funding, administration, or operation of an intelligence activity within the responsibility and authority of the Director of National Intelligence involving classified information, but does not include differences of opinions concerning public policy matters." *Id.* at § 3033(k)(5)(G)(i).

In addition, the law requires the Inspector General of the Intelligence Community within 14 calendar days to determine whether information with respect to an urgent concern "appear[s] credible." *Id.* at § 3033(k)(5)(B). The law does

not require that the complaint be based on first-hand information.

During this reporting period, the Center received whistleblower disclosures, made referrals to other divisions and agencies, reviewed reports of urgent concern, and evaluated requests for External Review Panels. The Center also arranged and participated in several community outreach events, including site visits to various Intelligence Community Hotline Programs, and community discussions for the implementation of *Intelligence Authorization Act for Fiscal Years 2018, 2019, and 2020*, § 5333 and § 5334. Additionally, the Center organized an outreach event on November 20, 2019, at the ODNI Headquarters in McLean, Virginia in recognition of International Fraud Awareness Week. During the event, IC IG staff emphasized the importance of reporting suspected fraud, waste, and abuse, and provided an overview of the Center. The staff also highlighted current IC IG professional opportunities and shared resource materials to advise ODNI personnel on how to contact the IC IG Hotline.

THE INSPECTOR GENERAL COMMUNITY

This year marks the 42nd anniversary of the *Inspector General Act of 1978*. President Jimmy Carter signed the Act, and described the new statutory Inspectors General as "perhaps the most important new tools in the fight against fraud." The Office of the Inspector General of the Intelligence Community, one of 74 Inspectors General collectively overseeing the operations of nearly every aspect of the federal government, looks forward to continuing to work with the Council of the Inspectors General on Integrity and Efficiency (CIGIE) on important issues that significantly affect productivity, transparency, and accountability throughout the federal government.

Oversight.gov

Oversight.gov provides a "one stop shop" to follow the ongoing oversight work of all Offices of Inspectors General (OIGs) that publicly post reports. CIGIE manages the website on behalf of the Federal Inspector General community. The IC IG, like other OIGs, posts reports to its own website as well as to *Oversight.gov* to afford users the benefits of the website's search and retrieval features. *Oversight.gov* allows users to sort, search, and filter the site's database of public reports from all CIGIE member OIGs to find reports of interest. In addition, the site features a user-friendly map that allows users to find reports based on geographic location, and contact information for each OIG's hotline. Users can receive notifications when new reports are added to the site by following @OversightGov, CIGIE's Twitter account.

IC IG PROGRAMMATIC OBJECTIVES

In previous Semiannual Reports, the IC IG identified five programmatic objectives that served as measures by which the IC IG categorized its projects and activities. These areas were selected after a comprehensive review of reports, including the *2019 U.S. National Intelligence Strategy*; the *Consolidated Intelligence Guidance for Fiscal Years 2020-2024*; the *IC2025 Vision and Foundational Priorities*; the Office of the Inspector General of the Intelligence Community's *Management and Performance Challenges for the Office of the Director of National Intelligence*, as well as Management and Performance Challenges for the Central Intelligence Agency, Defense Intelligence Agency, National Geospatial-Intelligence Agency, National Reconnaissance

Office, and the National Security Agency; the Government Accountability Office's High Risk Series reports; and the Council of the Inspectors General on Integrity and Efficiency FY 2018 report, *Top Management and Performance Challenges Facing Multiple Federal Agencies.*

The objectives, established in early 2019, are again recognized in this *Semiannual Report*. The IC IG has selected the following five programmatic objectives to focus upon:

1. Improving the Efficiency and Effectiveness of the Intelligence Community's Cyber Posture, Modern Data Management, and IT Infrastructure.
2. Enhancing Workforce Management.
3. Championing Protected Disclosures.
4. Improving Oversight of Artificial Intelligence.
5. Integrating the Intelligence Community.

1 Improving the Efficiency and Effectiveness of the Intelligence Community's Cyber Posture, Modern Data Management, and IT Infrastructure

The Intelligence Community has identified cybersecurity as one of its most important priorities, as reflected in the 2019 National Intelligence Strategy, the DNI's IC2025 Vision and Foundational Priorities, the 2018 Management and Performance Challenges for the Office of the Director of National Intelligence (ODNI), and budget requests spanning multiple fiscal years. Ongoing and future IC IG projects selected will review and evaluate the effectiveness of ODNI's information security and the cohesiveness of cyber and information technology (IT) integration across the Intelligence Community.

AUD-2019-004: Fiscal Year 2019 Independent Evaluation of the Office of the Director of National Intelligence's Information Security Program and Practices as Required by the *Federal Information Security Modernization Act of 2014*

The Audit Division completed an evaluation to assess the effectiveness and maturity of ODNI's information security program and practices for Fiscal Year 2019, as required by the *Federal Information Security Modernization Act of 2014* (FISMA). FISMA requires an annual independent evaluation of federal agencies' information security programs and practices. The IC IG performed this evaluation using the *FY 2018 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics* developed by the Office of Management and Budget, Department of Homeland Security, and the Council of the Inspectors General on Integrity and Efficiency. The IC IG issued two recommendations for improving ODNI's information security program and practices. In addition to these recommendations, prior IC IG reports include 20 information security-related recommendations that remain open.

The IC IG collected the Executive Summaries and metric results from the Intelligence Community elements' FY 2018 FISMA reports and provided them to the Office of Management and Budget. In accordance with the *Federal Information Security Modernization Act*, the Director of the Office of Management and Budget is responsible for summarizing FISMA reports from the Intelligence Community elements and submitting an annual report to Congress on the effectiveness of information security policies and practices relating to national security systems.

Additional details are listed in the classified Annex of the IC IG's Semiannual Report.

AUD-2019-003: Office of the Director of National Intelligence's Implementation of the *Cybersecurity Information Sharing Act of 2015*

The Audit Division completed an audit of the Office of the Director of National Intelligence's implementation of the *Cybersecurity Information Sharing Act of 2015 (*CISA). The audit's objective was to assess the actions taken over the prior, most recent, two-year period to carry out CISA requirements.

On December 18, 2015, Congress passed Public Law 114-113, the *Consolidated Appropriations Act of 2016*, which includes Title I - the *Cybersecurity Information Sharing Act of 2015.*[1] CISA was established to improve cybersecurity in the United States through enhanced sharing of cyber threat information.[2] CISA creates a framework to facilitate and promote the voluntary

sharing of cyber threat indicators[3] and defensive measures[4] among and between Federal and non-Federal entities.[5]

CISA requires the inspectors general of the "appropriate Federal entities," defined as the Departments of Commerce, Defense, Energy, Homeland Security, Justice, and the Treasury, and the ODNI, "in consultation with the Inspector General of the Intelligence Community and the Council of Inspectors General on Financial Oversight," to jointly report to Congress by December 18 – every two years – on the actions taken over the most recent two-year period to carry out CISA.[6] The results, presented in this ODNI report, were included in the joint, biennial report provided to Congress in December 2019.

IC IG auditors concluded that ODNI's sharing of cyber threat indicators and defensive measures with Intelligence Community elements has improved over the past two years and efforts are underway to expand accessibility to information. Sharing cyber threat indicators and defensive measures increases the amount of information available for defending systems and networks against cyber attacks. In April 2017, the Intelligence Community Security Coordination Center (IC SCC) deployed a capability – the Intelligence Community Analysis and Signature Tool (ICOAST) – to increase sharing of cybersecurity threat intelligence at the top secret security level. According to the Director of IC SCC, the deployment of ICOAST has enabled cyber analysts to more rapidly share high-quality cyber threat information and has enabled analytic collaboration. In Calendar Year (CY) 2017 and CY 2018, components continued to share cyber threat information through various reporting means, including email, written reports, and websites. In addition, efforts are underway to further enhance accessibility to cyber threat information and reports.

The report also addressed CISA reporting requirements, to include: information sharing policies and procedures, classification of shared information, the timeliness of sharing, and barriers to sharing. The report did not include any recommendations.

Additional details are listed in the classified Annex of the IC IG's Semiannual Report.

[1] The *Cybersecurity Information Sharing Act of 2015* is codified at 6 U.S.C. § 1501 *et seq*.

[2] "Cybersecurity threat" is broadly defined to include an action 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. The term "cyber threat information" is used in this report to refer to both cyber threat indicators and defensive measures.

[3] According to 6 U.S.C. § 1501(6), cyber threat indicators include threat-related information such as methods of defeating or causing users to unwittingly enable the defeat of security controls and methods of exploiting cybersecurity vulnerabilities.

[4] According to 6 U.S.C. § 1501(7)(A), defensive measures include an action, device, procedure, 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 vulnerability.

[5] A Federal entity is a department or agency of the United States or any component of such department or agency. 6 U.S.C. § 1501(8). Non-Federal entities include state, local, and tribal governments; private sector companies; and academic institutions. Federal entities can share cybersecurity information with one another and with non-Federal entities, and non-Federal entities can share cybersecurity information with one another and with Federal entities. 6 U.S.C. § 1501(14).

[6] 6 U.S.C. § 1506(b)(1).

AUD-2019-005-U: Joint Report on the Implementation of the *Cybersecurity Information Sharing Act of 2015*

The Offices of the Inspectors General (OIGs) for the Departments of Energy, Homeland Security, Justice, Defense, Commerce, Energy, and the Treasury, and the ODNI, assessed the implementation of the *Cybersecurity Information Sharing Act of 2015* for Calendar Years (CY) 2017 and 2018. The objective of the assessment was to review the actions taken over the prior, most recent, two-year period to carry out the requirements of CISA.

On December 18, 2015, Congress passed Public Law 114-113, the *Consolidated Appropriations Act, 2016*, which includes Title I – the *Cybersecurity Information Sharing Act of 2015* (CISA).[7] CISA was established to improve cybersecurity in the United States through enhanced sharing of cyber threat information.[8] CISA creates a framework to facilitate and promote the voluntary sharing of

cyber threat indicators[9] and defensive measures[10] among and between Federal and non-Federal entities.[11]

CISA requires the inspectors general of the "appropriate Federal entities," defined as the Departments of Commerce, Defense, Energy, Homeland Security, Justice, and the Treasury, and the ODNI, "in consultation with the Inspector General of the Intelligence Community and the Council of Inspectors General on Financial Oversight," to jointly report to Congress by December 18 – every two years – on the actions taken over the most recent two-year period under the statute.[12] This report meets the joint, biennial reporting requirement.

The OIGs determined that sharing of cyber threat indicators and defensive measures has improved over the past two years within their respective agencies and efforts are underway to expand accessibility to information. Sharing cyber threat indicators and defensive measures increases the amount of information available for defending systems and networks against cyber attacks. In April 2017, the Intelligence Community Security Coordination Center (IC SCC) deployed a capability – the Intelligence Community Analysis and Signature Tool (ICOAST) – to increase sharing of cybersecurity threat intelligence at the top secret security level. According to the Director of IC SCC, the deployment of ICOAST has enabled cyber analysts to more rapidly share high-quality cyber threat information and has enabled analytic collaboration. Also, in CY 2017 and CY 2018, entities continued to share cyber threat information through various reporting means, including email, written reports, and websites. In addition, efforts are underway to further enhance accessibility to cyber threat information and reports included in ICOAST. Given the availability of the secret and unclassified government computing clouds, IC SCC is in the planning and development stages for the deployment of ICOAST instances at the secret and unclassified security classification levels, with the goal of operating at those security classification levels by the end of 2019. Although progress has been made to improve cyber threat information sharing, using the Automated Indicator Sharing (AIS) remains a challenge.[13] Specifically, the number of non-governmental entities using AIS is minimal, and other challenges with AIS information deter its use.

Concerning the specific areas that the statute requires be assessed and reported on by the OIGs, the auditors determined that the "appropriate Federal entities" continue to implement the statute.[14] Specifically, the OIGs determined that the "appropriate Federal entities" responsible for sharing, receiving, or disseminating cyber threat information:

- Use policies and procedures that are sufficient (*i.e.*, the policies and procedures met the legislative requirements of the statute), with the exception of five Department of Defense (DoD) components.
- Properly classify cyber threat indicators and defensive measures.
- Authorize security clearances for the specific purpose of sharing cyber threat indicators or defensive measures with the private sector.
- Appropriately disseminate cyber threat information that had been shared by Federal and non-Federal entities, and appropriately used that information.
- Share cyber threat indicators and defensive measures in a timely and adequate manner and with appropriate entities.
- Receive cyber threat indicators and defensive measures in a timely and adequate manner.
- Use the Department of Homeland Security capability – AIS – to receive cyber threat indicators or defensive measures, with the exception of six DoD components and ODNI.
- Did not receive information that was unrelated to a cybersecurity threat that included personal information of a specific individual or information identifying a specific individual.
- Did not receive notices due to a failure to remove information not directly related to a cybersecurity threat that was personal information of a specific individual.

- Did not need to take steps to minimize adverse effects on the privacy and civil liberties of United States persons from activities carried out under CISA because there were no known adverse effects.
- Identified barriers that have hindered sharing of cyber threat indicators and defensive measures, to include:
  - Restrictive classifications limit cyber threat information from being widely shared.
  - Inability of machines to communicate with each other reduces the speed at which cyber threat information sharing occurs.
  - Uncertainty about the protection from liability provided by CISA impacts the willingness of private sector entities to share cyber threat information.
  - Challenges with AIS information that deter its use.

[7] *See supra* note 1.

[8] *See supra* note 2.

[9] *See supra* note 3.

[10] *See supra* note 4.

[11] *See supra* note 5.

[12] *See supra* note 6.

[13] AIS is the capability developed by the Department of Homeland Security as required by CISA from which the Federal Government receives cyber threat information in real-time that has been made available by non-Federal entities.

[14] 6 U.S.C. § 1506(b)(2).

INS-2019-003: ODNI's Oversight of Intelligence Community Major Systems Acquisition Cybersecurity Risks

During the reporting period, the Inspections and Evaluations Division concluded an evaluation of the efficiency and effectiveness of the existing authorities, policies, and processes applicable to the Office of the Director of National Intelligence's oversight of Intelligence Community (IC) Major Systems Acquisition (MSA) cybersecurity risks. *The Intelligence Reform and Terrorism Prevention Act of 2004* (IRTPA) empowered the Director of National Intelligence with milestone decision authority for Intelligence Community Major Systems Acquisition. IRTPA also requires a program management plan for each National Intelligence Program MSA that includes cost, schedule, performance goals, and program milestone criteria. The DNI is directed to periodically review and assess the plans and present the results to Congress. The review identified inconsistencies in oversight process and stakeholder involvement, opportunities for improving cybersecurity education and training focused on the IC acquisition workforce, and a lack of consistency in defining terms.

2 Enhancing Workforce Management

The IC IG established this objective based on the Right, Trusted, Agile Workforce foundational priority as identified in the Director of National Intelligence's IC2025 Vision and Foundational Priorities and the People enterprise objective outlined in the National Intelligence Strategy. The projects highlighted below contribute to this priority by ensuring that the workforce has the necessary tools to carry out the mission of the Intelligence Community.

Security Clearance Initiatives

An effective and efficient government-wide personnel security clearance process helps ensure that relevant security information is identified and assessed in a timely manner to enable agencies to recruit and retain qualified and trusted employees and contractors. Executive Order 13467 assigns the Director of National Intelligence responsibility, as the Security Executive Agent, for the development, implementation, and oversight of effective, efficient, and uniform policies and procedures governing the conduct of investigations and adjudications for eligibility for access to classified information and to hold a sensitive position. The Director of National Intelligence has instituted a variety of reform efforts designed to improve background investigation and adjudication timeliness and improve the quality of information used to make security clearance decisions, compile system-wide metrics, and assess and oversee personnel security program implementation across the Executive Branch. Despite these reform efforts, the processing of security clearances within the IC has been a longstanding and continuing challenge.

To appropriately plan oversight work on this critical challenge, the IC IG reviewed information concerning policies and practices for reporting on the security clearance process. Based on the IC IG's review, during Fiscal Year 2020 the IC IG initiated two projects. The Audit Division initiated an audit of the integrity and use of security clearance data reported to ODNI by the CIA, DIA, Department of State, FBI, NGA, NRO, NSA, and the ODNI. The objectives of the audit are to determine whether IC elements accurately capture, document, and report required security clearance processing timeliness information; IC elements calculate processing timeliness in a consistent manner; the Security Executive Agent accurately complies and reports data provided by the IC elements, as required; and whether the Security Executive Agent uses timeliness data to address security clearance backlog and inform security clearance-related policy decisions.

Concurrently, the Inspections and Evaluations Division initiated an evaluation of the Intelligence Community's implementation of security clearance reciprocity in accordance with Security Executive Agent Directive (SEAD) 7, *Reciprocity of Background Investigations, and National Security Adjudications*. The objective of the evaluation is to assess security clearance reciprocity determinations made by the CIA, DIA, Department of State, FBI, NGA, NRO, NSA, and the ODNI. The evaluation will determine whether IC elements review security clearance databases to determine whether prior or current background investigations or national security eligibility adjudications exist for incoming personnel; determine whether IC elements accept background investigations completed by authorized investigative agencies that meet all or part of the investigative requirements for a national security background investigation,

except for allowed exceptions in SEAD 7; determine whether IC elements accept national security eligibility adjudications conducted by authorized adjudicative agencies at the same or higher level, except for allowed exceptions in SEAD 7; determine whether IC elements make and record reciprocity determinations for national security background investigations and adjudications in a timely manner; and identify additional means to promote efficiency and effectiveness of security clearance reciprocity in the IC.

INS-2020-003: Evaluation of ODNI Senior Executive Service (SES) Reporting

In response to § 6727 of the *Intelligence Authorization Act for Fiscal Years 2018, 2019, and 2020*, which was included as Division E of the *National Defense Authorization Act for Fiscal Year 2020* (the Act), the Office of the Inspector General of the Intelligence Community's Audit Division and Inspections and Evaluations Division jointly initiated a project to report on the Senior Executives in the Office of the Director of National Intelligence. Specifically, the Act requires that the IC IG submit to the congressional intelligence committees a report that includes: the number of required SES positions for the ODNI; whether such requirements are reasonably based on the mission of the ODNI; and a discussion of how the number of SES positions in the ODNI compares to the number of senior positions at comparable organizations.

To facilitate the discussion related to comparable organizations, the IC IG requested Senior Executive Service (SES) position information from CIA, DIA, NSA, NRO, NGA, the Office of the Under Secretary of Defense for Intelligence, and ODNI. The data collected was assessed against ODNI metrics to identify similarities in the SES position span of control ratios and to make SES organizational structure comparisons. In order to help determine whether ODNI's requirements are reasonably based on the mission of the ODNI, the team extracted mission data from organizational webpages and conducted interviews with ODNI staff to discuss their framework for making mission need determinations. Due to the short timeline associated with this review, data collection, research, and more detailed statistical analysis had to be limited. The review is ongoing and the IC IG anticipates releasing its final report during the fourth quarter of Fiscal Year 2020.

3 Championing Protected Disclosures

Intelligence Community employees and contractors collect and analyze information to develop the most accurate and insightful intelligence possible on external threats to our national security. These Intelligence Community professionals serve in a classified work environment in which information about intelligence programs and activities is not available for public review, which makes their duty to lawfully disclose information – or blow the whistle – regarding potential wrongdoing, including fraud, waste, abuse, and corruption, that much more critical to the oversight process.

Whistleblowing is the lawful disclosure to an authorized recipient of information a person reasonably believes evidences wrongdoing. It is the mechanism to relay the right information to the right people to counter wrongdoing and promote the proper, effective, and efficient performance of the Intelligence Community's mission. Whistleblowing in the IC is extremely important as it ensures that personnel can "say something" when they "see something" through formal reporting procedures without harming national security and without retaliation.

To support this effort, the IC IG established the Center for Protected Disclosures (The Center). The Center covers three functional areas critical for whistleblowers in the Intelligence Community.

First, the Center receives and processes whistleblower complaints through the IC IG's Hotline program. The Hotline program receives whistleblower complaints and concerns through public and secure telephone numbers and website addresses as well as walk-in meetings at the IC IG's main office in Reston, Virginia, and its satellite offices in McLean, Virginia, and Bethesda, Maryland. The Center also receives complaints filed via drop boxes located in various ODNI facilities.

The Hotline program also receives and processes allegations of "urgent concerns" disclosed pursuant to the *Intelligence Community Whistleblower Protection Act* (ICWPA). The ICWPA established a process to ensure that the Director of National Intelligence, the Senate Select Committee on Intelligence, and the House Permanent Select Committee on Intelligence receive disclosures of allegedly serious or flagrant problems, abuses, violations of law or executive order, or deficiencies relating to the funding, administration, or operation of an intelligence activity. The Center tracks all ICWPA disclosures, ensures review of materials for classified information, and coordinates disclosures with other Inspectors General for appropriate review and disposition. During the reporting period, the IC IG transmitted one ICWPA disclosure to the DNI, which was subsequently provided to the Senate Select Committee on Intelligence, and the House Permanent Select Committee on Intelligence.

Second, the Center provides guidance to individuals seeking more information about the options and protections afforded to individuals who may wish to make a protected disclosure to the IC IG and/or Congress, or who believe they have suffered reprisal because they made a protected disclosure. The IC IG also conducts community outreach and training activities to ensure stakeholders present and receive accurate and consistent whistleblowing information relating to these and other matters.

During this reporting period, the Center visited six IC element OIG's Hotline Programs where representatives discussed potential challenges, Hotline process, and information in an effort to

continue to increase the effectiveness of the IC IG's Hotline program and the implementation of the *Intelligence Authorization Act for Fiscal Years 2018, 2019, and 2020*, § 5334. The Center intends to continue this effort.

Third, the Center administers requests by employees and contractors in the Intelligence Community for the IC IG to review their allegations of reprisal under Presidential Policy Directive 19 (PPD-19), *Protecting Whistleblowers with Access to Classified Information,* and under section 1104 of the *National Security Act of 1947* (50 U.S.C. § 3234) and section 3001(j)(1) of the *Intelligence Reform and Terrorism Prevention Act of 2004* (50 U.S.C. § 3341(j)). PPD-19 and its codifying statues protect employees serving in the IC and those who are eligible for access to classified information by prohibiting reprisal for reporting fraud, waste, and abuse, while protecting classified national security information. The IC IG has important responsibilities when handling reprisal claims, including the administration of external review processes to examine allegations of whistleblower reprisal. An individual who believes they have suffered reprisal for making a protected disclosure and who has exhausted their agency's review process for whistleblower reprisal allegations may request an External Review Panel (ERP).[15] Upon exhaustion of those processes and a request for review, PPD-19 permits the IC IG to exercise its discretion to convene an ERP to conduct a review of the agency's determination.

During this reporting period, the IC IG, in coordination with our Forum partners from the Department of Energy and the Department of Treasury OIGs completed an ERP. The ERP reviewed the submission by the requestor, collected additional evidence, and conducted interviews concerning allegations raised in the ERP request. The ERP members determined the local Agency OIG's investigation was correct that the Agency did not reprise against the requestor in violation of PPD-19 and that they would have taken the same actions absent the requestor's protected disclosures.

The IC IG received five new ERP requests during the current reporting period, which are under review. The Center conducts an initial assessment and review of materials submitted by both the complainant and the complainant's employing agency prior to reaching a determination. The IC IG is currently conducting initial assessments of ten ERP requests; five of the ten were initiated during the previous reporting period.

---

[15] Previously only appearing in PPD-19, section C, during the reporting period Congress codified External Review Panels in the *Intelligence Authorization Act for Fiscal Years 2018, 2019, and 2020.* 50 U.S.C. § 3236.

INS-2019-004: Intelligence Community Directive 701

There is a need to clearly distinguish between whistleblowers and those individuals who make unauthorized disclosures by taking it upon themselves to decide what classified information should be disclosed to the public. Whistleblowers make use of formal reporting procedures that will protect both the classified information and the whistleblower. Any disclosure of classified information falling outside of these established procedures constitutes an unauthorized disclosure – not protected whistleblowing – and falls into the realm of insider threat behavior. Unauthorized disclosures put sensitive operations and intelligence sources and methods at risk. In addition, failing to effectively address unauthorized disclosures reduces the incentive for the IC's workforce to use formal reporting procedures to make protected disclosures to report allegations of fraud, waste, or abuse involving classified information.

Intelligence Community Directive (ICD) 701, *Unauthorized Disclosure of Classified Information*, governs the Intelligence Community's efforts to deter, detect, report, and investigate unauthorized disclosures of classified national security information. The policy directs the Intelligence Community to accomplish these tasks by training personnel, developing comprehensive personnel security programs, conducting audits of system monitoring, and devising other appropriate measures to deter and detect unauthorized disclosures. Additional requirements are to conduct

preliminary inquiries, provide notifications and reports to appropriate authorities, and conduct investigations as required.

The IC IG's Inspections and Evaluations Division initiated a compliance inspection of the IC's implementation of ICD 701. The inspection will collect information from 17 IC elements to help establish a baseline assessment of required unauthorized disclosure mitigation activities and determine whether these activities adhere to the requirements identified in ICD 701.

The inspection process will then focus on reviewing guidance and oversight by identifying audit and system monitoring practices, training and personnel security programs, or other actions used to comply with ICD 701 policy requirements. The inspection will determine whether IC elements have incorporated processes for stakeholder notifications, reporting of preliminary inquiries, and conducting investigations in accordance with policy requirements. The compliance inspection of ICD 701 is ongoing.

In a parallel effort, the Investigations Division continued work related to its ICD 701 responsibilities. These efforts included outreach and liaison discussions related to the status of ICD 701 reporting programs, formalizing reporting processes to ensure that appropriate notifications are made in a timely fashion, and engaging in benchmarking efforts to identify obstacles to appropriate implementation. The liaison and outreach efforts included multiple IC elements and leveraged the expertise and institutional knowledge from all agencies and elements.

4 Improving Oversight of Artificial Intelligence

Data is one of the cornerstones of work conducted by Offices of Inspectors General. Whether text dense criteria documents or structured databases of transactional and financial data, Offices of Inspectors General face mounting challenges in finding, sorting, and analyzing vast amounts of data. The IC IG selected artificial intelligence as an objective for review due to the presence it has played in multiple ODNI documents and published reports. In the Augmenting Intelligence using Machines (AIM) Initiative, former Director of National Intelligence Daniel Coats identified artificial intelligence as a vehicle to increase mission capability and enhance data interpretation throughout the IC.

As noted in two previous Semiannual Reports, the IC IG is coordinating Intelligence Community Offices of Inspectors Generals' efforts to identify both the opportunities and challenges machine learning and artificial intelligence present. In light of the Director of National Intelligence's *IC2025 Vision and Foundation Priorities'* "Augmenting Intelligence using Machines (AIM)" initiative, the IC IG is continuing foundational actions to build general awareness and common understanding among IC oversight authorities in the following areas:

- **Building a Community of Interest:** Drawing from the interest expressed by participants in the "Making Better Use of Data: Automation, Analytics, and AI" break-out session at the 2019 Intelligence Community Inspectors General Annual Conference, the IC IG has begun exploring the viability of establishing an Intelligence Community Offices of Inspectors General Community of Interest (CoI) as a forum for follow-on discussion. The IC IG began to leverage the perspectives of 30 session participants who expressed their interest in future collaboration. These participants represent 11 Intelligence Community Offices of Inspectors General as well as management elements of the FBI. Their work spans eight distinct functional areas: Audit, Data Analytics, Front Office, Forensic Analysis, Inspections and Evaluations, Investigations, Management and Administration, and Overseas Contingency Operations Oversight. Their input will continue to help shape how the CoI is formed and how it relates to the Intelligence Community Inspectors General Forum and the Council of the Inspectors General on Integrity and Efficiency (CIGIE) and their subordinate entities having shared areas of interest.
- **Enhancing individual and collective understanding:** The IC IG continues to explore opportunities for Offices of Inspectors General to advance their understanding of this transformative field, and their capabilities to audit, investigate, inspect, and evaluate its implementation. The IC IG has engaged subject matter experts and stakeholders across the Intelligence Community, the federal government, academia, and industry to begin mapping the landscape of AIM-related research, planning, implementation, and governance activities. The IC IG continued follow-up discussions with the ODNI AIM Champion, the IC Artificial Intelligence Ethics Working Group, and the Intelligence and National Security Alliance. The IC IG also participated in and applied insights developed from the 2019 annual IC Machine Learning Conference, the annual IC/NRO Big Data Forum, the National Intergovernmental Executive Forum's AI Roundtable, the annual IC Science and

Technology Portfolio Showcase, and data analysis/visualization user groups within the intelligence and defense communities.

- **Developing criteria and measures:** The IC IG has begun to compile a listing of existing and projected efforts being pursued under the aegis of the AIM initiative. Combined with the IC IG's concurrent efforts to identify and leverage ongoing discussions across government, industry, and advocacy groups about artificial intelligence governance, the IC IG will advance the ability of Intelligence Community Offices of Inspectors General to develop criteria and measures for evaluating investments in oversight of artificial intelligence in terms of personnel, training, and technology.
- **Information exchanges and collaboration:** The IC IG has sustained its expanded outreach efforts and engagements of CIGIE's Data Analytics Working Group and Emerging Technology Subcommittee. The IC IG continues its work to enable shared situational awareness within the Inspector General community, both in the Intelligence Community and the broader federal government.
- **Education and training resources:** The IC IG continues to research and compile an initial list of government and academic entities with existing classes, courses, and seminars that could substantively broaden and deepen the expertise of Intelligence Community Offices of Inspectors General in addressing data and artificial intelligence-related issues and topics. We established encouraging new dialogue with the National Intelligence University's Data Science faculty. This conversation focused on the potential for leveraging its expertise in designing training curricula for IG staff drawn from the range of existing courses offered across the Intelligence Community. The IC IG will share the results of these efforts for consideration by the Intelligence Community Inspectors General Forum, CIGIE's Professional Development Committee, CIGIE's Emerging Technology Subcommittee, and the CIGIE Training Institute for discussion and expansion.

5 Integrating the Intelligence Community

The IC IG identified integrating the Intelligence Community as a programmatic objective because it is fundamental to ODNI's mission and national security. When created by the Intelligence Reform and Terrorism Prevention Act of 2004, ODNI was given the responsibility to improve information sharing and ensure integration across the IC. Strategic prioritization, coordination, and deconfliction of IC collection, analysis, production, and dissemination of national intelligence are essential to optimizing IC resource management, and decision-making, and to accomplishing ODNI's mission. ODNI's Integrated Mission Strategy for 2019-2023 and the National Intelligence Strategy identified developing collaborative collection and analysis capabilities, as well as sharing and safeguarding information, as enduring challenges.

INS-2019-002: The Intelligence Community's Foreign Language Program

In February 2019, the IC IG's Inspections and Evaluations Division initiated an evaluation of the effectiveness of the Office of the Director of National Intelligence's execution of enterprise management responsibilities and functions related to the Intelligence Community Foreign Language Program (ICFLP). The ICFLP was established at Congressional direction by the *Intelligence Authorization Act of Fiscal Year 2005* with the mission "to improve the education of IC personnel in foreign languages critical in meeting the long-term intelligence needs of the United States." The Director of National Intelligence implemented this mandate through Intelligence Community Directive (ICD) 630, *Intelligence Community Foreign Language Capability*, establishing an "integrated approach to develop, maintain, and improve foreign language capabilities across the IC."

This evaluation marks the first Inspector General review of the ICFLP since its inception. The Inspections and Evaluations Division examined how the Office of the Director of National Intelligence has progressed in meeting Congressional requirements and whether the Director is managing the Intelligence Community foreign language enterprise in an integrated manner. The Inspections and Evaluations Division examined advocacy for budgetary resources and linking allocations to impacts, outcomes against foreign language strategic objectives, and governance effectiveness. The Inspections and Evaluations Division engaged with foreign language program process owners, partners, and stakeholders in the ODNI, CIA, DIA, FBI, NGA, NSA, and the Office of the Undersecretary of Defense for Intelligence. The review encompassed Fiscal Years 2005 through 2019 in achieving IC mission objectives. The IC IG anticipates releasing its final report in the fourth quarter of Fiscal Year 2020.

The Intelligence Community Information Sharing Working Group

Since September 11, 2001, the President, Congress, independent commissions, and think tanks have placed greater emphasis on the need for information sharing within the Intelligence Community. *The Intelligence Reform and Terrorism Prevention Act of 2004* and Executive Order 12333 assigned the Director of National Intelligence authorities and responsibilities to provide oversight of the Intelligence Community; this includes the development of guidelines for

how information or intelligence is provided to or accessed by the Intelligence Community.

In 2019, the Intelligence Community Inspectors General Forum's Inspections Committee Intelligence Oversight Working Group recommended a joint review be conducted of the Director of National Intelligence's implementation of intelligence and information sharing responsibilities. The Inspections and Evaluations Division currently plans to conduct an evaluation of Intelligence Community Information Sharing in Fiscal Year 2021.

The Inspections and Evaluations Navigator Training Tool

The Inspections and Evaluations (I&E) Division continued to partner with CIGIE to develop and deploy the I&E Navigator training tool pilot project. This is the cornerstone of the CIGIE Training Institute's initial venture into web-based instruction. The I&E Navigator is an online web-based performance support system that is both integrated with instruction and used as a stand-alone, on-demand workplace resource for Inspections and Evaluations professionals.

When fielded and integrated with CIGIE's performance-focused design and leading-edge learning, I&E Navigator will provide on-demand access to Offices of Inspectors General. It will augment and replace the current formal, in-person classroom delivery model. Over time, CIGIE plans to develop and field similar training and performance enhancing support systems for the Investigation and Audit Committees.

The IC IG's interest in the project stems from the dual goals of leveraging the I&E Navigator tool to enhance its own on-boarding training and operations support needs, and to serve as the Intelligence Community's champion for making it available on classified networks as a means to address common needs.

During this reporting period the IC IG's referent for the tool participated in two pilot offerings of online, interactive I&E Navigator training: "Jump Start" in October 2019, and "Driving" between January and February 2020. These engagements helped inform leadership perspectives of the IC IG and CIGIE's Training Institute on provisions necessary to make I&E Navigator uniformly available on computer systems most commonly used by Intelligence Community Offices of Inspectors General. In March 2020, the CIGIE Training Institute made "Jump Start" training available to the Intelligence Community Inspectors General Forum's Inspections and Evaluations members, supporting participation from home during the COVID-19 reduced staffing period.

The Five Eyes Intelligence Oversight and Review Council

The former Inspector General of the Intelligence Community, along with the Inspectors General from the United States Department of Justice, National Geospatial-Intelligence Agency, and National Security Agency, attended the October 2019 annual meeting of the Five Eyes Intelligence Oversight and Review Council, hosted by the United Kingdom's Investigatory Powers Commissioner's Office. The Council meets annually, with the host country rotating among the participants.

Five Eyes Intelligence Oversight and Review Council Annual Meeting in London

The Council is composed of the following non-political intelligence oversight, review, and security entities of the Five Eyes countries: the Office of the Inspector-General of Intelligence and Security of Australia; the Office of the Communications Security Establishment Commissioner and the National Security and Intelligence Review Agency of Canada; the Office of the Inspector-General of

Intelligence and Security of New Zealand; the Investigatory Powers Commissioner's Office of the United Kingdom; and the Office of the Inspector General of the Intelligence Community of the United States.

The exchange of views and best practices among the Five Eyes continues to be an important mechanism for information sharing. Throughout the meeting, participants provided an overview of key issues facing their organizations, and addressed transparency; the importance of independence; legislative changes; and joint oversight. The United States' delegation facilitated discussions on the challenges of overseeing artificial intelligence and machine learning; information sharing between Five Eyes partners; and methods used by various oversight authorities during parallel investigations and reviews.

European Union - United States Privacy Shield

In September 2019, the former Inspector General of the Intelligence Community participated in the third annual review of the European Union – United States Privacy Shield framework held in Washington, D.C. Operational since August 2016, the Privacy Shield regulates and protects personal data transferred from the European Union to the United States for commercial purposes. The terms of the Privacy Shield require an annual review by the European Commission.

Senior United States government officials from the Office of the Director of National Intelligence, and United States Departments of Commerce, Justice, State, and Transportation joined with representatives from the European Union to review privacy issues, compliance monitoring, surveillance activities, and artificial intelligence. The former Inspector General provided an overview of the work conducted by inspectors general in the United States, and the relevance they play in the protection of the rule of law. In preventing and deterring waste, fraud, and abuse, inspectors general are obligated to generate public trust through independence and transparency.

The European Commission published its findings of the review in October 2019, stating that the United States continues to protect personal data transferred under the Privacy Shield. However, during the reporting period there was pending litigation in the European Court of Justice that challenges key components of the EU-US Privacy Shield. The final disposition of this case could affect the viability of the Privacy Shield and change how data sharing agreements are structured.

ODNI Management Challenges

In September 2019, the IC IG issued what it considered to be the most significant management and performance challenges facing the ODNI, the Office of the Director of National Intelligence's Management and Performance Challenges. The report was included in the FY 2019 Agency Financial Report, published in November 2019.

The *Reports Consolidation Act of 2000* requires that the Inspector General of the Intelligence Community identify the most serious management and performance challenges facing the Office of the Director of National Intelligence. Based on findings from audits, inspections, and investigations, and through the IC IG's position as the Chair of the Intelligence Community Inspectors General Forum, the IC IG concludes that the most serious management and performance challenges facing ODNI are in the following areas:

1. Reforming the Security Clearance Process;
2. Strengthening Information Security and Management;
3. Enhancing Intelligence Community Coordination, Integration, and Information Sharing;
4. Producing Auditable Financial Statements;
5. Improving Management of the Office of the Director of National Intelligence's Workforce; and

6. Strengthening the Office of the Director of National Intelligence's Management of its Policies.

Additional details are listed in the classified Annex of the IC IG's *Semiannual Report*.

Intelligence Community Management Challenges

The Office of the Inspector General of the Intelligence Community issued a Capstone Report summarizing shared management and performance challenges faced by the Intelligence Community during Fiscal Year 2019. In accordance with *The Reports Consolidation Act of 2000*, federal agencies' Inspectors General must prepare a report summarizing what the Inspectors General consider to be the most serious management and performance challenges facing their agencies, and briefly assess the organization's progress in addressing those challenges. Based on audits, inspections, and investigations conducted during the previous fiscal year, the Inspectors General in the Intelligence Community each prepared their own report identifying challenges.

The IC IG worked together with the Inspectors General from the Central Intelligence Agency, the Defense Intelligence Agency, the National Geospatial-Intelligence Agency, the National Reconnaissance Office, and the National Security Agency to prepare a consolidated Capstone report that identifies the most significant shared challenges, which relate to the following areas (not presented in order of importance):

1. Strengthening Information System Security and Management;
2. Countering Insider Threats;
3. Strengthening Acquisition and Contract Management;
4. Producing Auditable Financial Statements;
5. Improving Workforce Management;
6. Reforming the Security Clearance Process;
7. Managing Internal and Interagency Relationships; and
8. Championing Protected Disclosures.

In addition, Inspectors General are monitoring the need for oversight authorities to stay current with the transformative powers of cognitive technologies, particularly artificial intelligence (AI) and machine learning. As a result, the six Offices of Inspectors General also identified managing AI as an emerging challenge.

Additional details are listed in the classified Annex of the IC IG's *Semiannual Report*.

INTELLIGENCE COMMUNITY INSPECTORS GENERAL FORUM

One of the most significant ways the Office of the Inspector General of the Intelligence Community works to improve the integration of the Intelligence Community is through the Intelligence Community Inspectors General Forum (the Forum). By statute, the Forum consists of the twelve statutory or administrative Inspectors General with oversight responsibility for an element of the IC. The Inspector General of the Intelligence Community is the Chair of the Forum.

The Forum serves as a mechanism through which members can learn about the work of individual members that may be of common interest, and discuss questions about jurisdiction or access to information and staff. As Chair, the Inspector General of the Intelligence Community leads the Forum by coordinating efforts to find joint solutions to mutual challenges for improved integration among the Forum members. Forum committees, topic-specific working groups, and subject matter experts generate ideas to address shared concerns and mutual challenges for consideration and decision by the Inspectors General.

In addition to meetings of the Forum, the IC IG's Principal Deputy Inspector General, Assistant Inspectors General, the Counsel to the IG, and Director of the Center for Protected Disclosures each chair committees to further collaboration, address common issues affecting Inspectors General equities, implement joint projects, support and participate in Inspectors General training, and disseminate information about best practices. These committees and topic-specific working groups meet regularly. Summaries of the Forum and committee meetings held during the reporting period follow.

INTELLIGENCE COMMUNITY INSPECTORS GENERAL FORUM

The Intelligence Community Inspectors General Forum held two meetings during the reporting period. In December, the Forum discussed potential artificial intelligence initiatives with the Council of the Inspectors General on Integrity and Efficiency, private sector organizations, and with foreign partners in conjunction with the Five Eyes Oversight and Review Council. Additionally, the Chief of ODNI's Office of Civil Liberties, Privacy, and Transparency briefed Forum members on the Intelligence Community's Artificial Intelligence Ethics Working Group. The session concluded with an update by two inspectors general (IGs) who serve on CIGIE's Professional Development Committee. The IGs shared with the Forum professional opportunities available to all members of the Inspector General community.

Inspectors General focused on emerging issues of great significance to the Intelligence Community.

The Forum convened again in March. The session focused primarily on congressional directives and the *Intelligence Authorization Act for Fiscal Years 2018, 2019, and 2020*. The Forum will continue to meet quarterly, with the next meetings scheduled in June, September, and December 2020.

DEPUTIES COMMITTEE

The Deputies Committee gathered three times during the reporting period. In December, the Assistant Director of National Intelligence for Human Capital joined the Deputies to discuss the Intelligence Community Joint Duty Program. The group explored innovative ideas for increasing awareness about Joint Duty Assignments, hiring and training opportunities, and addressed the unique needs of the Inspector General community.

The Deputies Committee explored innovative opportunities for Offices of Inspectors General.

The Deputies Committee assembled in February, and again in March, to examine provisions in the *Intelligence Authorization Act for Fiscal Years 2018, 2019, and 2020*. Their findings were discussed in further detail with the Intelligence Community Inspectors General Forum.

AUDIT COMMITTEE

In December 2019, the Audit Division hosted the Audit Committee and Cybersecurity Subcommittee quarterly meeting to discuss multiple topics of community interest. The meeting included two guest speakers from the Government Accountability Office (GAO), who presented the unique challenges of providing oversight of artificial intelligence (AI). The GAO presentation was open to attendance by OIG investigators and inspectors. The quarterly meeting also included a guest speaker from the CIA OIG who served as the Chair of the Federal Audit Executive Committee Peer Review Workgroup. The speaker provided an update on the federal External Peer Review Guide. Federal audit organizations are required to have an external peer review every three years. With the revision of Generally Accepted Government Auditing Standards (the Yellow Book), a workgroup was formed to update the External Peer Review Guide. Given the number of IC elements scheduled to perform or receive a peer review, the timing of the presentation was helpful. The quarterly meeting also featured a speaker from the IC IG who shared the outcome of joint work performed by the Offices of Inspectors General of the Departments of Energy, Homeland Security, Justice, Defense, Commerce, Energy, Treasury, and the Office of the Director of National Intelligence (ODNI), concerning the actions taken over the most recent two-year period to carry out the *Cybersecurity Information Sharing Act.*

In March 2020, the Audit Division planned the Audit Committee and Cybersecurity Subcommittee quarterly meeting to feature the ODNI's Chief, Office of Civil Liberties, Privacy, and Transparency and his presentation on the ethics of 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. The quarterly meeting was also scheduled to have sessions to discuss the requirements for addressing the *Intelligence Authorization Act for Fiscal Years 2018, 2019, and 2020* requirement to assess Classification; the status of revisions to the OIG metrics for performing the *Federal Information Security Modernization Act* evaluation; and to highlight the issuance of the *Intelligence and Cybersecurity Subcommittee Consolidated Chief Information Officer Cybersecurity Performance Evaluation Measures Report for Fiscal Year 2019.* The March 2020 quarterly meeting was postponed due to COVID-19.

The Audit Committee addressed the unique challenges of providing oversight of artificial intelligence, revisions to the federal External Peer Review Guide, and results of joint work required by the *Cybersecurity Information Sharing Act.*

COUNSELS COMMITTEE

The Counsels Committee meets regularly to discuss legal and policy issues of common interest to the IC, and to promote the consistent interpretation of statutes, regulations, policies, and Executive Orders. The Counsels Committee operates with the goal of providing legal analysis of, and options relating to, issues of particular importance to the Forum for final decision making.

Counsels led discussions to respond to requirements set forth by the *Intelligence Authorization Act for Fiscal Years 2018, 2019, and 2020.*

During this reporting period, the Counsels Committee discussed and, when appropriate, collaborated on key initiatives, including the following:

The Counsels Committee met several times to discuss the *Intelligence Authorization Act for Fiscal Years 2018, 2019, and 2020*. The Counsels' discussions focused on how to improve the processing of whistleblower complaints and how to best harmonize whistleblower processes and procedures.

The Counsels Committee established two working groups with IC IG and representatives from the Intelligence Community Inspectors General Forum to address and respond to congressionally directed actions within the *Intelligence Authorization Act*. The two working groups focused on how best to accomplish the requirements and direction contained in § 5333, *Harmonization of Whistleblower Processes and Procedures*; § 5334, *Oversight by Inspector General of the Intelligence Community Over Intelligence Community Whistleblower Matters*; and § 6713, *Review of Intelligence Community Whistleblower Matters*.

In addition, IC IG Counsel's Office conducted briefings and facilitated discussion on provisions in the *Intelligence Authorization Act* to the Intelligence Community Inspectors General Forum and to the Deputies Committee.

INSPECTIONS AND EVALUATIONS COMMITTEE

The Inspections and Evaluations Committee led a dialogue with attendees on their Fiscal Year 2020 work plans, as well as common challenges and projects that could be conducted jointly or concurrently. The Acting Assistant Inspector General for the Inspections and Evaluations Division also shared with the Committee ongoing and future Division projects.

During this reporting period, the Inspections and Evaluations Committee received numerous briefings from ODNI, Intelligence Community, and federal Offices of Inspectors General (OIG) on a wide variety of topics of interest. The IC IG's Training and Workforce Development Office provided attendees with an update on the 2020 Intelligence Community Inspectors General Conference, to include insight into considerations for conference break-out rooms and topics. The Inspections and Evaluations Committee, in coordination with the Audit Committee, planned to host the Chief of ODNI's Office of Civil Liberties, Privacy, and Transparency for a briefing on ethics in artificial intelligence.

In March 2020, additional briefings were scheduled with the Council of the Inspectors General on Integrity and Efficiency's (CIGIE's) Blue Book Working Group efforts to revise the CIGIE Quality Standards for Inspections and Evaluations Programs, and CIGIE's Peer Review Guide Working Group. The briefings were intended to provide an update on CIGIE's efforts to revise the *Guide for Conducting External Peer Reviews of I&E Organizations of Federal Offices of Inspector General*. Due to COVID-19, the briefings were cancelled and will be rescheduled at a future date.

Culminating a collaborative effort by two Committee members to present a "lessons learned" document to enhance future joint reviews of controlled access programs, Inspections and Evaluations Division staff presented attendees with the draft tri-fold pamphlet of collaboratively developed tradecraft tips for conducting projects on controlled access programs (or other activities with special controls). The pamphlet will be disseminated to the wider Intelligence Community Inspectors General Forum for comment prior to publication and distribution.

The Inspections and Evaluations Committee worked across the Intelligence Community to address issues important to Offices of Inspectors General.

The Inspections Committee also led a discussion of the language contained in the *Intelligence Authorization Act for Fiscal Years 2018, 2019, and 2020*, § 6721, "IG Reports on Classification Status." The Committee's discussion focused on requirements to coordinate agency OIG objectives to allow for more succinct capstone reporting on the collective IC enterprise. Committee attendees agreed to discuss collaboration opportunities at the next Committee meeting in the 4th Quarter of Fiscal Year 2020.

INVESTIGATIONS COMMITTEE

The Intelligence Community Inspectors General Forum's Investigations Committee met on two occasions during this reporting period. In November 2019, the Committee discussed various investigative procedures, the possibility and benefit of having a community wide case management tracking system, investigative techniques related to reprisal investigations, and best investigative practices within the Community. Additionally, the Committee discussed resources that were disseminated during its December 2019 engagement related to Intelligence Community Directive (ICD) 701, *Unauthorized Disclosure of Classified Information*. Those resources included Fact Sheets, a list of Frequently Asked Questions, and internal workflow graphics.

The Investigations Committee focused on increasing collaborative investigations, identifying de-confliction strategies in the case of overlapping areas of responsibility, and the impact of a centralized repository.

During its March 2020 meeting, the Investigations Committee covered topics of collaborative investigative efforts to aid in identifying trends and suspected irregularities in investigations and the benefits of sharing information. The Committee also continued its discussion on identifying de-confliction strategies in the case of overlapping areas of responsibility.

The Investigations Committee also led discussions regarding the implementation and potential impact of a centralized repository as indicated in the *Intelligence Authorization Act for Fiscal Years 2018, 2019, and 2020*, particularly § 5334. The Committee's discussion focused on possible procedures and processes required to submit information to the IC IG, the impact of sharing personal identifying information, exercising unilateral jurisdiction, the need for a shared information management tool, and other required collaborative efforts.

MANAGEMENT AND ADMINISTRATION COMMITTEE

The Management and Administration Committee engaged on the topics of professional development, strategic workforce planning, and records management. The group welcomed representatives from the Intelligence Community Human Capital Office who provided an overview of the Office of the Director of National Intelligence's Multi-Sector Workforce (MSW) initiative, highlighting the program's objectives, the legal implications associated with implementation, how agencies and elements are applying Multi-Sector Workforce across the community, aligning MSW with strategic workforce planning, and best practices for adopting and employing MSW effectively. Rounding out the discussion on human capital planning and management, the NGA OIG Career Services team shared information on their Career Development Initiative, resulting in a healthy information exchange on career development best practices and opportunities for greater collaboration amongst the Forum OIGs with a focus on improving employee recruitment, development, and retention. Among the opportunities discussed were building a coalition and establishing a community of practice for IC OIG career development, piloting an effort to examine Joint Duty within the IC OIG community, establishing a fellows program akin to the CIGIE Fellows Program for IC OIG professionals, and the potential for virtual Joint Duty Assignments. The group also received an update on the Office of Management and Budget/ National Archives and Records Administration's guidance on transitioning to electronic records, including key implementation milestones.

The Management and Administration Committee collaborated with Intelligence Community leadership to explore the enhancement of professional opportunities for personnel within the Inspector General community.

WHISTLEBLOWER COMMITTEE

The Whistleblower Committee continues to monitor impending legislative changes.

In March 2020, the Whistleblower Committee planned to meet concerning recent changes in law implementing the *Intelligence Authorization Act for Fiscal Years 2018, 2019, and 2020*, § 5333 and § 5334, and the standards of review used by IC IG in evaluating requests for External Review Panels under Presidential Policy Directive 19, Section C. This March 2020 meeting was postponed due to COVID-19.

INTELLIGENCE COMMUNITY DATA ANALYTICS COMMUNITY OF INTEREST WORKING GROUP

The Office of the Inspector General of the Intelligence Community hosted the fifth session of the Intelligence Community Data Analytics Community of Interest Working Group. The Working Group meets semiannually and includes members of the Intelligence Community Inspectors General Forum. The Working Group was established to explore and share ideas on data collection and analysis, enhance insights into trends and risks, and improve operations to identify potential waste, fraud, and abuse. Representatives from DIA OIG, NGA OIG, NSA OIG, NRO OIG, the Department of Justice OIG, and the IC IG attended and participated in the discussions.

Representatives from the Department of Justice OIG Data Analytics Office provided the group an overview of their current contract risk assessment model, lessons learned and improvements to the model. The IC IG extended the offer to continue these discussions and related topics of interest.

The Intelligence Community Data Analytics Community of Interest Working Group discussed oversight of artificial intelligence using data, contract risk assessment models, data collection, and analysis when identifying potential waste, fraud, and abuse in the federal government.

RECOMMENDATIONS SUMMARY

Following publication of an inspection report, the IC IG's Inspections and Evaluations Division interacts with the inspected elements at least quarterly to ensure actions are taken to implement report recommendations. A description of the actions are entered into the IC IG's recommendations tracking database. Inspections and Evaluations leadership has the responsibility for approving the closure of a recommendation once it has been demonstrated that responsive actions have met the intent of a recommendation. The Inspections and Evaluations Division may revisit closed recommendations to ensure there is no slippage or back-tracking in their fulfillment or to inform follow-on reviews.

For the ODNI to realize the maximum benefit from IC IG audits, management should ensure that adequate corrective action is taken in a timely manner to address audit recommendations. The Audit Division closely monitors implementation of its recommendations through continuous communication with stakeholder points of contact on progress and actions. The status of open recommendations is periodically conveyed to ODNI senior managers. The Audit Division issues a memorandum for formal closure when it determines that all recommendations in a report have been addressed.

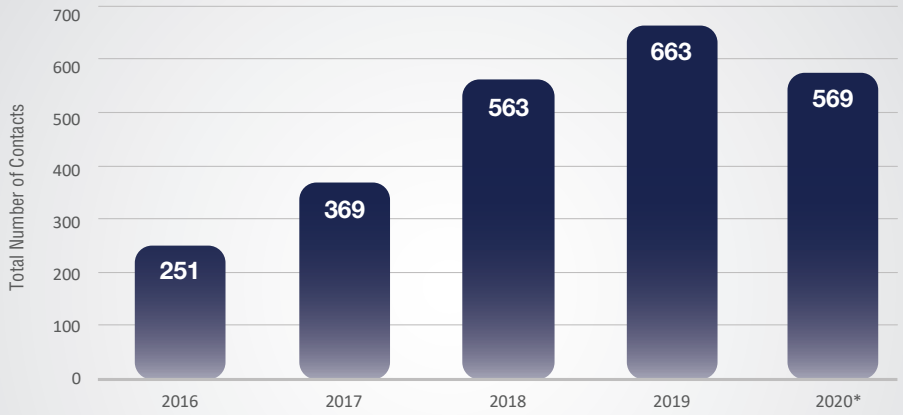
Report Name	Date Issued	Total Issued	New This Period	Closed This Period	Currently Open
FY 2020					
Audit: FY 2019 Independent Evaluation of Federal Information Security Modernization Act (FISMA)	October	2	2	0	2
Inspection: ODNI's Oversight of Intelligence Community Major Systems Acquisition Cybersecurity Risks	November	6	6	0	6
FY 2019					
Audit: Office of the Director of National Intelligence's Fiscal Year 2018 Conference Spending	September	2	0	0	2
Audit: Management of Privileged Users of Office of the Director of National Intelligence Information Systems	September	9	0	0	9
Inspection: Assessment of the ODNI Methods Used to Substantiate Post-Secondary Education Claims Made by ODNI Employees Subsequent to Entry-on-Duty	August	7	0	2	5
Audit: FY 2018 Independent Evaluation of Federal Information Security Modernization Act (FISMA)	February	11	0	0	10
Inspection: Cyber Threat Intelligence Integration Center	January	9	0	0	7
FY 2018					
Inspection: IC Freedom of Information Act (FOIA) Programs	September	10	0	1	3
Audit: Memorandum to the Chief Operating Officer re: Charge Card Program	August	2	0	0	1
Inspection: Assessment of IC Information System Deterrence, Detection, and Mitigation of Insider Threats	March	4	0	0	1
FY 2017					
Inspection: Assessment of ODNI Information System Deterrence, Detection, and Mitigation of Insider Threats	September	19	0	3	1
FY 2012					
Audit: Study: Intelligence Community Security Clearance Reciprocity	December	2	0	1	0
	Totals	**83**	**8**	**7**	**47**

IC IG HOTLINE

ICIG HOTLINE
Report suspected fraud, waste, and abuse
Open: 855-731-3260 • www.dni.gov/ICIG
Secure: 933-2800 • https://go.ic.gov/hotline

The IC IG Hotline provides a confidential means for Intelligence Community employees, contractors, and the public to report information concerning suspected fraud, waste, and abuse of programs and activities within the responsibility and authority of the Director of National Intelligence. The Hotline can be contacted via classified and unclassified email and phone lines, U.S. mail, secure web submissions, walk-ins, and drop boxes located in select ODNI facilities.

IC IG NEW CONTACTS LOGGED BY FISCAL YEAR



*Includes data for half FY, from October 2019-March 2020

NEW CONTACTS LOGGED THIS REPORTING PERIOD*

569

*Due to COVID-19, only urgent contacts were logged during the last two weeks of March 2020. All other contacts received during this period will be reflected in the following SAR.

METHODS OF CONTACT

Phone Calls	1,214
Email/Web	412
USPS Mail	31
Faxes	12

ABBREVIATIONS AND ACRONYMS

AI ..... Artificial Intelligence
AIM..... Augmenting Intelligence using Machines
AIS ..... Automated Indicator Sharing
The Center ..... The Center for Protected Disclosures
CIA..... Central Intelligence Agency
CIGIE ..... Council of the Inspectors General on Integrity and Efficiency
CISA..... Cybersecurity Information Sharing Act of 2015
CoI..... Community of Interest
CY ..... Calendar Year
DHS..... Department of Homeland Security
DIA ..... Defense Intelligence Agency
DNI ..... Director of National Intelligence
DoD..... Department of Defense
ERP ..... External Review Panel
FBI ..... Federal Bureau of Investigation
FISMA ..... Federal Information Security Modernization Act of 2014
FOIA ..... Freedom of Information Act
The Forum..... Intelligence Community Inspectors General Forum
FY ..... Fiscal Year
GAO ..... Government Accountability Office
HPSCI ..... House Permanent Select Committee on Intelligence
I&E..... Inspections and Evaluations
IC..... Intelligence Community
ICD..... Intelligence Community Directive
ICFLP..... Intelligence Community Foreign Language Program
IC IG..... Inspector General of the Intelligence Community
ICOAST..... Intelligence Community Analysis and Signature Tool
IC SCC ..... Intelligence Community Security Coordination Center
ICWPA ..... Intelligence Community Whistleblower Protection Act
IG ..... Inspector General
IPERA ..... Improper Payments Elimination and Recovery Act
IRTPA ..... Intelligence Reform and Terrorism Prevention Act of 2004
ISCM..... Information Security Continuous Monitoring

IT.....Information Technology
MSA.....Major Systems Acquisition
MSD.....Mission Support Division
MSW..... Multi-Sector Workforce
NGA..... National Geospatial-Intelligence Agency
NRO..... National Reconnaissance Office
NSA..... National Security Agency
ODNI..... Office of the Director of National Intelligence
OIG.....Office of the Inspector General
PPD..... Presidential Policy Directive
SEAD..... Security Executive Agent Directive
SES.....Senior Executive Service
SSCI..... Senate Select Committee on Intelligence
U.S. .....United States
U.S.C. .....United States Code

Office of the Inspector General of the Intelligence Community

571-204-8149 open; 939-9200 secure