

UNCLASSIFIED

DIRECTOR OF NATIONAL INTELLIGENCE
WASHINGTON, DC



INTELLIGENCE COMMUNITY POLICY MEMORANDUM 504 (01)

MEMORANDUM FOR DISTRIBUTION

SUBJECT: Intelligence Community Policy Framework for Commercially Available Information

REFERENCES:

- A. National Security Act of 1947, as amended
- B. Federal Information Security Modernization Act
- C. Privacy Act of 1974
- D. Federal Agency Data Mining Reporting Act of 2008, 42 U.S.C. Sec. 2000EE-3(b)(1)
- E. Electronic Communications Privacy Act, 18 U.S.C. Sec. 2702
- F. Cybersecurity Information Sharing Act, 6 U.S.C. Sec. 1503
- G. Executive Order 12333, United States Intelligence Activities
- H. Intelligence Community Directive 503, Intelligence Community Information Environment Risk Management, 25 October 2024
- I. Committee on National Security Systems Instruction No. 1253, Security Categorization and Control Selection for National Security Systems
- J. Committee on National Security Systems Instruction No. 1253F Attachment 6, Privacy Overlay
- K. ODNI Memorandum ES 2024-00744, Implementing Guidance on the Intelligence Community Policy Framework for Commercially Available Information, 6 May 2024
- L. Intelligence Community Policy Framework for Commercially Available Information, May 2024

A. Purpose

1. This Intelligence Community Policy Memorandum (ICPM) governs the access to and collection and processing of Commercially Available Information (CAI) by elements of the Intelligence Community (IC), as defined by Reference A.

2. This ICPM is to be read in conjunction with ES 2024-00744, *Implementing Guidance on the Intelligence Community Policy Framework for Commercially Available Information*, 6 May

UNCLASSIFIED

SUBJECT: Intelligence Community Policy Framework for Commercially Available Information ICPM 504 (01)

2024, or follow-on guidance, and rescinds and replaces Reference B of that document, *Intelligence Community Policy Framework for Commercially Available Information*, May 2024.

B. Definitions

1. For the purposes of this policy, definitions may be found in the Appendix.

C. Policy

1. Overview

a. Commercial entities are collecting and aggregating unprecedented amounts of personal data through networked computing applications. This data comes from a variety of sources including cell phones, cars, household appliances, and other personal devices. Some of these commercial entities make such information available to a diverse set of purchasers, including for-profit and non-profit entities, foreign adversaries, and domestic and transnational organizations.

b. Like these other purchasers, elements of the IC lawfully access, collect, and process such CAI in pursuit of mission imperatives, and the information often provides critical intelligence value.

c. At the same time, these datasets can reveal sensitive and intimate personal details and activities. The IC's access to and collection and processing of this information is subject to numerous laws and policies governing intelligence activities, which include those found in the Constitution; statutes such as the Federal Information Security Modernization Act and the Privacy Act of 1974; Executive Order 12333; IC element procedures approved by the Attorney General for the protection of U.S. persons' information pursuant to Section 2.3 of Executive Order 12333 ("Attorney General Guidelines"); and other relevant policies and procedures, such as those promulgated by the Office of Management and Budget. Dedicated IC officials, including privacy and civil liberties, oversight, compliance, and legal officers, provide counsel and monitor compliance with these laws and policies.

d. This existing legal and regulatory regime protects privacy and civil liberties. However, the increasing availability of CAI and its potential sensitivity call for additional clarity in how the IC will make effective use of such information while ensuring that privacy and civil liberties remain appropriately protected. To those ends, the Director of National Intelligence issues this ICPM, which:

(1) In section C.2., establishes general principles governing the IC's access to and collection and processing of all CAI, as defined herein; and

(2) In section C.3., lays out a framework to govern the IC's access to and collection and processing of certain sensitive forms of CAI described in section C.3.a. (hereinafter "Sensitive CAI").

SUBJECT: Intelligence Community Policy Framework for Commercially Available Information ICPM 504 (01)

e. This ICPM is intended to augment each IC element's Attorney General Guidelines and related policies.¹ In doing so, it establishes a common baseline for how IC elements access, collect, and process Sensitive CAI; while allowing individual IC elements flexibility to experiment in the manner best suited to both meet the IC element's operational needs and protect privacy and civil liberties.²

2. General Principles for CAI: The principles in this section govern the IC's access to and collection and processing of all CAI and inform the more specific requirements for Sensitive CAI in section C.3.

a. IC elements' access to and collection and processing of CAI shall be authorized by and consistent with all applicable law and in furtherance of a validated mission or administrative need or function.

b. The protection of privacy and civil liberties, and compliance with procedures governing the conduct of intelligence activities, shall be integral considerations, timely considered, in an IC element's access to and collection and processing of CAI.

c. IC elements shall undertake reasonable efforts to determine the original source(s) of CAI they access or collect and the method(s) through which the CAI was generated and aggregated.

d. IC elements shall assess the integrity and quality of CAI they access or collect—including, as appropriate, by assessing whether the CAI reflects any underlying biases or inferences—in order to ensure that any intelligence products created with that data are consistent with applicable IC standards for accuracy and objectivity (with a focus on standards relating to the quality and reliability of the information).

e. IC elements shall not access, collect, or process CAI for the purpose of disadvantaging persons based on their ethnicity, race, gender, gender identity, sexual orientation, or religion; nor shall they access, collect, or process CAI for the purpose of taking adverse action against an individual based solely on that individual's exercise of

¹ This ICPM does not alter, replace, or limit any requirement found in any IC element's Attorney General Guidelines, including requirements for approval and for special circumstances collection. To the contrary, this ICPM provides the IC's standard approach to CAI and is not intended to conflict with an IC element's Attorney General Guidelines. To the extent an IC element's Attorney General Guidelines provide more stringent requirements than this ICPM, the Guidelines shall control.

² This ICPM governs the access to and collection and processing of CAI by elements of the IC, as defined by Reference A. IC elements within a department or agency are responsible for complying with this ICPM in addition to any applicable department or agency regulations and policies that are not otherwise inconsistent with this ICPM. In cases where an IC element within a department or agency accesses, collects, or processes CAI for mixed purposes—i.e., to jointly support its IC mission and other complementary departmental or agency missions and requirements—such IC element shall comply with the principles and requirements in this ICPM to the maximum extent practicable consistent with the mission requirements compelling the access to or collection or processing of such information.

SUBJECT: Intelligence Community Policy Framework for Commercially Available Information ICPM 504 (01)

constitutionally protected rights.

f. IC elements shall apply to CAI appropriate safeguards that are tailored to the sensitivity of the information—generally determined by the volume, proportion, and nature of information concerning U.S. persons—and its anticipated use. These safeguards shall reflect consideration of any newly available privacy enhancing methods or technologies and must ensure CAI is properly secured, handled appropriately, and subject to appropriate auditing, retention, destruction, and oversight requirements.

g. IC elements shall have in place appropriate processes for managing and periodically reviewing CAI, and any new uses of CAI, in order to ensure the fulfillment of mission or administrative needs and the proper implementation of safeguards and privacy-enhancing techniques.

h. To the extent appropriate and practicable, IC elements shall maintain and make available to other IC elements documentation regarding access to and the collection, processing, and safeguarding of CAI, in order to support oversight and promote visibility and learning across the Community on best practices.

i. The IC shall provide appropriate transparency to the public and relevant oversight entities on the policies and procedures governing its access to and collection and processing of CAI to further public understanding of intelligence activities while continuing to protect intelligence sources and methods and law enforcement sensitive information, as well as other privileged and operationally sensitive information.

3. Framework for Sensitive CAI

a. Scope of Application: Definition of Sensitive CAI.

(1) Establishing categorical distinctions between “sensitive” and “non-sensitive” data is challenging in a digital environment where the types and volume of data and processing methods to aggregate and draw insights from that data are expanding rapidly. Nevertheless, this ICPM is intended to establish a uniform baseline for all IC elements to categorize and handle CAI.

(2) Consistent with this objective, it is possible to identify conditions that elevate the sensitivity of CAI such that it should be brought within the scope of section C.3. of this ICPM. Specifically, CAI should be considered “Sensitive CAI” and subject to Section C.3. of this ICPM if it meets both the following criteria:

(a) The CAI is purchased from a commercial entity through a commercial transaction for a fee or made available by the commercial entity at no cost through a commercial transaction that normally would involve a fee (e.g., a free trial offering of CAI); and

(b) The CAI is known or reasonably expected to contain:

i. A substantial volume of personally identifiable information (PII) regarding U.S. persons; or

SUBJECT: Intelligence Community Policy Framework for Commercially Available Information ICPM 504 (01)

ii. A greater than de minimis volume of:

1. Sensitive data, which is defined as data that captures personal attributes, conditions, or identifiers that are traceable to one or more specific U.S. persons, either through the dataset itself or by correlating the dataset with other available information; and that concerns the U.S. person's or U.S. persons' race or ethnicity, political opinions, religious beliefs, sexual orientation, gender identity, medical or genetic information, financial data, or any other data the disclosure of which would have a similar potential to cause substantial harm, embarrassment, inconvenience, or unfairness to the U.S. person or U.S. persons described by the data; or

2. Data that captures the sensitive activities of U.S. persons or persons in the United States, with sensitive activities defined as activities that over an extended period of time establish a pattern of life; reveal personal affiliations, preferences, or identifiers; facilitate prediction of future acts; enable targeting activities; reveal the exercise of individual rights and freedoms (including the rights to freedom of speech and of the press, to free exercise of religion, to peaceable assembly—including membership or participation in organizations or associations—and to petition the government); or reveal any other activity the disclosure of which could cause substantial harm, embarrassment, inconvenience, or unfairness to the U.S. person or person in the United States who engaged in the activity.

(3) Notwithstanding the above criteria, Sensitive CAI does not include:

(a) Newspapers or other periodicals; weather reports; books, journal articles, or other published works; public filings or records; or similar documents or databases, whether accessed through a subscription or accessible free of cost; or

(b) Limited data samples made available so an IC element can evaluate whether to purchase the full dataset and not accessed, retained, or used for any other purpose unless assessed in accordance with section C.3.b. of this ICPM.

(4) Additionally, information that would otherwise qualify as Sensitive CAI under this ICPM is not subject to the requirements of this section if such information is accessed or collected for research and development purposes, but only if the following criteria are met: Office of the Director of National Intelligence (ODNI) is notified prior to the access or collection of the CAI; the access or collection is subject to the oversight of the IC element's Institutional Review Board or a similar mechanism; and the CAI is not accessed, retained, or used for any other purpose besides research and development unless assessed in accordance with section C.3.b. of this ICPM.

(5) All CAI accessed or collected, regardless of whether it constitutes Sensitive CAI, remains subject to other applicable laws and policies, including procedures approved by the Attorney General pursuant to section 2.3 of Executive Order 12333. Furthermore, IC elements retain the discretion to apply enhanced safeguards to any dataset containing information the IC element deems sensitive, regardless of whether the dataset would qualify as Sensitive CAI under this ICPM.

SUBJECT: Intelligence Community Policy Framework for Commercially Available Information ICPM 504 (01)

b. Access and Collection

(1) To ensure IC elements access and collect Sensitive CAI in a manner that promotes the efficient use of resources, protects privacy and civil liberties, and appropriately maintains operational security, IC elements shall have in place policies and procedures that, at a minimum, implement the following requirements:

(a) *Participation in the Procurement Process.* To the extent appropriate given operational security considerations, determinations to access or collect Sensitive CAI shall involve privacy and civil liberties officials, intelligence oversight officials, legal counsel, information officers, and other offices or components that possess relevant equities or experience.³

(b) *Analysis.* Before accessing or collecting Sensitive CAI, IC elements shall take the following steps:⁴

(i) *Mission or administrative need or function.* IC elements shall assess the Sensitive CAI to determine if it would support an authorized mission or administrative need or function. Determinations to access or collect Sensitive CAI should be guided by the nature, scope, reliability, and timeliness of the dataset required to fill the relevant requirement.

(ii) *Legal authority.* IC elements, through their assigned legal counsel, shall determine whether they have legal authority to access or collect the Sensitive CAI for the relevant supported requirement(s).

(iii) *Data sensitivity.* IC elements shall assess whether the dataset to be accessed or collected contains data that meets the criteria in section C.3.a.(2)(b). IC elements shall limit their access to and collection and processing of such data to the maximum extent feasible consistent with the need to fulfill the mission or administrative need or function.

(iv) *Privacy and civil liberties risks.* IC elements shall assess the privacy and civil liberties risks associated with accessing, collecting, or processing the Sensitive CAI, as well as how the IC element may be able to mitigate such risks. IC elements shall also consider whether the Privacy Act of 1974 is applicable.

(v) *Privacy-enhancing techniques.* IC elements shall assess whether the relevant mission or administrative requirement can be achieved if any reasonably available

³ When multiple IC elements seek to purchase Sensitive CAI as a group, the IC elements may choose to designate a lead IC element, or arrange for offices and components from all interested IC elements to participate in the procurement process.

⁴ It is possible that an IC element may learn information relevant to the analysis contemplated by this paragraph after procuring access to or collecting Sensitive CAI. IC elements are thus required to complete as much of the analysis required by section C.3.b.(1)(b) as feasible based on the information available to them before they make a decision to access or collect the Sensitive CAI. If the IC element learns information about the CAI after accessing or collecting it that would materially affect their prior analysis under this paragraph, they shall redo the analysis of relevant aspects and the overall assessment required by section C.3.b.(1)(b).

SUBJECT: Intelligence Community Policy Framework for Commercially Available Information ICPM 504 (01)

privacy-enhancing techniques, such as filtering or anonymizing, the application of traditional safeguards (to include access limitations and retention limits), differential privacy techniques, or other information masking techniques (such as restrictions or correlation), are implemented for information concerning U.S. persons.

(vi) *Data sourcing, integrity, and quality.* To the extent feasible given operational security considerations, IC elements shall undertake a reasonable effort to determine the original source(s) of the data in a Sensitive CAI dataset and the method through which the dataset was generated and aggregated, and whether any element of the IC previously accessed or collected the same or similar Sensitive CAI from the source. IC elements further shall assess the quality and integrity of the Sensitive CAI they intend to access or collect—including by, as appropriate, assessing whether the CAI reflects any underlying biases or inferences—in order to ensure that any intelligence products created with that data are consistent with applicable IC standards for accuracy and objectivity.

(vii) *Security risks.* IC elements shall assess the security, operational, and counterintelligence risks associated with the means of accessing or collecting the Sensitive CAI, as well as how the IC element may be able to mitigate such risks. In making such an assessment, IC elements shall, to the extent the information is reasonably available to them, take into account whether any other IC element previously accessed or collected the same or similar Sensitive CAI from the source.

(viii) *Overall assessment.* Based on the totality of the circumstances, IC elements shall determine whether the value of accessing or collecting the Sensitive CAI likely outweighs the privacy and civil liberties risks, data integrity and quality risks, security risks, and any other risks not detailed above, that cannot reasonably be mitigated.

(c) *Use of Assessments from Prior IC Access or Collection.* In undertaking the analysis described in section C.3.b.(1)(b), IC elements may, as appropriate, rely on the most recent privacy and civil liberties risk, data integrity and quality, and security risk assessments conducted by other IC elements with respect to the same Sensitive CAI. When relying upon assessments conducted by another IC element, IC elements remain individually responsible for compliance with this ICPM and their own regulations and policies.

(d) *Approval Process and Authority.* IC elements may access or collect Sensitive CAI only after receiving the approval of the IC element head. IC element heads may delegate this authority, as necessary. A delegation of this authority shall be documented in writing and specify that the delegee has the appropriate level of seniority to make the relevant determination. Before approving access to or collection of Sensitive CAI, the approving official must complete or review the analysis required by section C.3.b.(1)(b) and document the analysis and approval.

(e) *Exigent Circumstances.* IC elements may use procedures that differ from those contained in section C.3.b.(1)(a) to section C.3.b.(1)(d) if doing so is necessary due to exigent circumstances. If IC elements access or collect information under exigent circumstances,

SUBJECT: Intelligence Community Policy Framework for Commercially Available Information ICPM 504 (01)

they shall document the reasons for doing so and undertake the procedures contained in section C.3.b.(1)(a) to section C.3.b.(1)(d) promptly after access or collection. All activities in all circumstances must be carried out in a manner consistent with the Constitution and laws of the United States, applicable executive orders, and the IC element's Attorney General Guidelines.

c. Systems. Sensitive CAI must be retained and processed in systems that (1) ensure and verify the Sensitive CAI is appropriately secured, and (2) enable IC elements to effectively implement, manage, and audit, as practicable, the privacy and civil liberties protections for Sensitive CAI required by this ICPM. To achieve this objective, Sensitive CAI activities are subject to the following system requirements:

(1) Authority to Operate. Sensitive CAI shall be maintained in systems used or operated by an IC element or by a contractor of an IC element with authority to operate (ATO).⁵ All systems should implement the applicable privacy control baseline to achieve ATO.⁶ These standards apply regardless of data volume or the manner of collection—to include Sensitive CAI datasets ingested directly from a commercial vendor; Sensitive CAI obtained from another part of the U.S. Government or third party; or extracts of Sensitive CAI exported from a data environment operated by a commercial vendor.

(2) Privacy Overlay. IC elements that maintain Sensitive CAI shall apply security and privacy controls necessary to protect PII and reduce privacy risks to individuals throughout the information lifecycle. When IC elements maintain Sensitive CAI on National Security Systems, they shall, where feasible and consistent with applicable requirements, apply security and privacy controls that, at a minimum, implement the Moderate Privacy Overlay control set.⁷

(3) Vendor Systems. IC elements shall, to the greatest extent feasible, ensure that commercial vendors' data repositories are subject to appropriate access restrictions, such as maintaining Sensitive CAI in a dedicated, secure enclave. In determining the appropriate manner of access to or collection of Sensitive CAI, IC elements shall take into account the security risks posed by a vendor company's systems architecture, safeguards, and possible access to or re-use of IC query terms.

d. Policies and Procedures for Safeguarding. IC elements shall have in place policies and procedures to ensure they appropriately safeguard any Sensitive CAI.⁸ To this end, such policies and procedures shall cover at a minimum:

⁵ Intelligence Community Directive 503, *Intelligence Community Information Environment Risk Management*, establishes IC policy for information technology systems security risk management, certification and accreditation.

⁶ Committee on National Security Systems Instruction No. 1253, *Security Categorization and Control Selection for National Security Systems*.

⁷ Committee on National Security Systems Instruction No. 1253F Attachment 6, Privacy Overlay.

⁸ IC elements shall also apply appropriate safeguards to Sensitive CAI obtained from another IC element, although they need not apply the exact same safeguards as the other IC element.

SUBJECT: Intelligence Community Policy Framework for Commercially Available Information ICPM 504 (01)

(1) Enhanced Safeguards. IC elements shall evaluate the existing safeguards afforded to any Sensitive CAI, given its authorized purpose and intended use, in order to determine whether enhanced safeguards are necessary to mitigate the assessed risk (as required by section C.3.b.(1)(b)). Such enhanced safeguards shall include one or more measures, such as those set forth below, identified by the IC element as appropriate and complementing the IC element's Attorney General Guidelines:

(a) Procedures to restrict access, including limiting the number of personnel with access and putting in place access controls, such as attribute-based access or other physical or logical access methods;

(b) Procedures for conducting and auditing queries, including potentially limiting the number of personnel who may run queries, establishing and enforcing standards for query predication, and requiring queries to be scoped as narrowly as possible consistent with mission requirements;

(c) A requirement to provide written justification and obtain the approval of a senior executive or other senior leader of the IC element prior to undertaking any queries, searches, or correlations of Sensitive CAI that are (1) intended to return known U.S. person information, or (2) reasonably likely to return a substantial volume of U.S. person information;

(d) Procedures to require the approval of a senior executive or other senior leader from the IC element when conducting queries or other searches of Sensitive CAI that constitute "data mining" according to the Federal Agency Data Mining Reporting Act of 2008, 42 U.S.C. § 2000EE-3(b)(1);

(e) Procedures to restrict dissemination, including requiring higher-level approval or legal review before or after U.S. person information is disseminated;

(f) Use of privacy-enhancing techniques, such as information masking that indicates the existence of U.S. person information without providing the content of the information, until the appropriate approvals are granted;

(g) Procedures for deleting U.S. person information in a result set returned in response to a query or other search of Sensitive CAI, unless the information is assessed to be associated or potentially associated with the documented mission-related justification for conducting the query or search; and

(h) Additional protective measures or training.

(2) Approval Process and Authority. IC element heads, in consultation with privacy and civil liberties officials, intelligence oversight officials, legal counsel, information officers, and other offices or components that possess relevant equities or experience, shall review and, where appropriate, approve the safeguards under this subsection. IC element heads may delegate this authority, as necessary. A delegation of this authority shall be documented in writing and specify that the delegate has the appropriate level of seniority to make the relevant determination.

SUBJECT: Intelligence Community Policy Framework for Commercially Available Information ICPM 504 (01)

e. Periodic Review and Reassessment. IC elements shall have in place policies and procedures that require review and re-evaluation to assess whether Sensitive CAI should be retained, and if so, whether existing safeguards are adequate. The appropriate periodicity of these re-evaluations will depend on the nature of the Sensitive CAI.

f. Data Management and Compliance. IC elements shall have in place policies and procedures that require a data management plan from the point of access or collection, throughout the data lifecycle, to disposition, based on an agency's information management policies (including, for example, a Records Control Schedule and, if U.S. person information is collected and retrieved, a System of Records Notice) or applicable law.

(1) Documentation. For all access to and collection and processing of Sensitive CAI, IC elements shall document, to the extent practicable and consistent with the need to protect intelligence sources and methods:

(a) The purpose of the access, collection, or processing, and intended uses of the Sensitive CAI;

(b) The nature or characterization, and volume, of the Sensitive CAI accessed or collected;

(c) The authority under which the Sensitive CAI is accessed, collected, or processed;

(d) The source of the Sensitive CAI and from whom the Sensitive CAI was accessed or collected;

(e) The mechanics of the access, collection, and processing (e.g., accessed at the vendor, ingested, data aggregated, raw data, analytics, etc.);

(f) Which organizational elements participated in the procurement process laid out in section C.3.b. and the analysis required by section C.3.b.(1)(b), and who approved the procurement under Section C.3.b.(1)(d);

(g) If applicable, the basis for relying on the emergency exception in section C.3.b.(1)(e);

(h) The policies and procedures for safeguarding applied under section C.3.d.;

(i) Whether an IC element has made unevaluated data or information available to any other IC elements or foreign partners and, if so, which IC elements or partners; and

(j) Any licensing agreements and/or contract restrictions applicable to the Sensitive CAI.

(2) Recordkeeping. IC elements shall maintain records containing the documentation required by section C.3.f.(1).

g. Reporting.

SUBJECT: Intelligence Community Policy Framework for Commercially Available Information ICPM 504 (01)

(1) Intelligence Community. Consistent with the protection of intelligence sources and methods, IC elements shall report on an annual basis to the ODNI CAI Leadership Team, led by the IC Open Source Intelligence (OSINT) Executive and composed of the Civil Liberties Protection Officer, the General Counsel, and the IC Chief Data Officer, or their designees, regarding the procurement of, access to, or collection of Sensitive CAI. These reports shall include:

(a) For every procurement of access to or collection of Sensitive CAI during the year, the documentation detailed in section C.3.f.;

(b) To further the consistent implementation of this ICPM, a description of why an IC element determined that accessed or collected CAI is not Sensitive CAI, in any circumstance when the IC element is aware that a different element deemed the same or similar CAI to be Sensitive CAI; and

(c) Upon request from the ODNI CAI Leadership Team, additional documentation about Sensitive CAI that an IC element has accessed, collected, or processed.

(2) To the maximum extent feasible and consistent with the protection of intelligence sources and methods, ODNI will make consolidated information from these annual reports available to all IC elements, in order to promote the efficient and effective use of Sensitive CAI and the consistent application of this ICPM.

(3) Public Transparency. Consistent with the *Principles of Intelligence Transparency for the Intelligence Community*, including the protection of intelligence sources and methods and law enforcement sensitive information, ODNI, in coordination with relevant IC elements, will keep Congress informed and shall provide a report to the public every two years regarding the IC's access to and collection, processing, and safeguarding of Sensitive CAI.

D. Roles and Responsibilities

1. The heads of IC elements shall:

- a. Establish and maintain policies and procedures implementing this ICPM;
- b. Implement processes to review and, where appropriate, approve the access to, collection, processing, and safeguarding of Sensitive CAI, unless the IC element head delegates such authority in a manner consistent with this ICPM;
- c. Maintain the documentation required by section C.3.f. and, consistent with section C.3.g., provide such documentation to ODNI; and
- d. Provide to ODNI copies of the policies and procedures required by this ICPM, and any information ODNI considers necessary for the report in section C.3.g.(3) to the extent consistent with the protection of intelligence sources and methods.

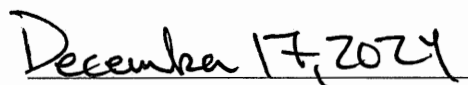
2. The OSINT Executive, as the senior ODNI official responsible for implementation of this ICPM, will:

SUBJECT: Intelligence Community Policy Framework for Commercially Available Information ICPM 504 (01)

- a. Make available to the IC consolidated information regarding the implementation of this ICPM, as required by section C.3.g.(2); and
- b. Report annually to Congress on the IC's access to and collection, processing, and safeguarding of Sensitive CAI, consistent with section C.3.g.(3).
- c. Provide a report to the public every two years on the IC's access to and collection, processing, and safeguarding of Sensitive CAI, as required by section C.3.g.(3).



Avril D. Haines



Date

SUBJECT: Intelligence Community Policy Framework for Commercially Available Information ICPM 504 (01)

Appendix

For the purposes of this ICPM:

“**Access**” means the viewing or examining of information for official purposes, or establishing the capability to view or examine information for official purposes (e.g., by purchasing a license), where the information viewed or examined is not stored or otherwise maintained under the control of the IC element.

“**Collection**” means the receipt of information by an IC element for official purposes, whether or not the information is retained. Collected information includes information received by any means, including information that is volunteered to the IC element. Collected information does not include: (a) information that is accessed by an IC element employee but is not stored or otherwise maintained under the control of the IC; or (b) information obtained from another IC element that has been lawfully provided by that IC element pursuant to its procedures.

“**Commercially Available Information**” means any data or other information that is of a type customarily made available or obtainable and sold, leased, or licensed to members of the general public or to non-governmental entities for purposes other than governmental purposes. CAI also includes data and information for exclusive government use knowingly and voluntarily provided by, procured from, or made accessible by corporate entities at the request of a government entity or on their own initiative.⁹

“**Personally Identifiable Information**” means information that can be used to distinguish or trace an individual’s identity, either alone or when combined with other information that is linked or linkable to a specific individual. For example, location information associated with a U.S. person’s mobile device over an extended period of time shall be treated as PII if the location information can be correlated with other available information to identify a specific natural person associated with the mobile device.

“**Process**” means the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, or disposal of information.

“**Publicly Available Information**” means information that has been published or broadcast for public consumption, is available on request to the public, is accessible online or otherwise to the public, is available to the public by subscription or purchase, could be seen or heard by any casual observer or member of the public, is made available at a meeting open to the public, or is observed by visiting any place or attending any event that is open to the public.

“**Sensitive Activities**” include activities that over an extended period of time establish a pattern of life; reveal personal affiliations, preferences, or identifiers; facilitate prediction of future acts;

⁹ For the purposes of this ICPM, CAI does not include data and information: obtained by the government pursuant to legal process; voluntarily provided to law enforcement by a corporate entity where such disclosures are made pursuant to a specific statutory scheme such as the Electronic Communications Privacy Act, 18 U.S.C. § 2702, or the Cybersecurity Information Sharing Act, 6 U.S.C. § 1503; or obtained from activities undertaken through human sources or through human-enabled means.

SUBJECT: Intelligence Community Policy Framework for Commercially Available Information ICPM 504 (01)

enable targeting activities; reveal the exercise of individual rights and freedoms (including the rights to freedom of speech and of the press, to free exercise of religion, to peaceable assembly—including membership or participation in organizations or associations—and to petition the government); or reveal any other activity the disclosure of which could cause substantial harm, embarrassment, inconvenience, or unfairness to the U.S. person or person in the United States who engaged in the activity.

“**Sensitive CAI**” means any information meeting the criteria in section C.3.a.

“**Sensitive Data**” includes data that captures personal attributes, conditions, or identifiers that are traceable to one or more specific U.S. persons, either through the dataset itself or by correlating the dataset with other available information; and that concerns the U.S. person’s or U.S. persons’ race or ethnicity, political opinions, religious beliefs, sexual orientation, gender identity, medical or genetic information, financial data, or any other data the disclosure of which would have a similar potential to cause substantial harm, embarrassment, inconvenience, or unfairness to the U.S. person or U.S. persons described by the data.

“**U.S. Person**” shall have the same meaning as it has in Executive Order 12333.

SUBJECT: Intelligence Community Policy Framework for Commercially Available Information ICPM 504 (01)

Distribution:

Director, Central Intelligence Agency
Director, Defense Intelligence Agency
Director, National Geospatial-Intelligence Agency
Director, National Reconnaissance Office
Director, National Security Agency
Under Secretary for Intelligence and Security, Department of Defense
Under Secretary for Intelligence and Analysis, Department of Homeland Security
Executive Assistant Director for Intelligence, Federal Bureau of Investigation
Assistant Secretary for Intelligence and Research, Department of State
Assistant Secretary for Intelligence and Analysis, Department of the Treasury
Chief of Intelligence, Drug Enforcement Administration
Director, Office of Intelligence and Counterintelligence, Department of Energy
Deputy Chief of Staff for Intelligence, United States Army
Director of Intelligence, United States Marine Corps
Director of Naval Intelligence, United States Navy
Deputy Chief of Staff for Intelligence, Surveillance and Reconnaissance, United States Air Force
Deputy Chief of Space Operations for Intelligence, United States Space Force
Assistant Commandant for Intelligence, United States Coast Guard
Director for Intelligence, Joint Chiefs of Staff, Department of Defense