



DEPARTMENT OF HOMELAND SECURITY
OFFICE *of* INTELLIGENCE *and* ANALYSIS

POLICY MANUAL

— 2025 —

UNCLASSIFIED

U.S. Department of Homeland Security
Office of Intelligence and Analysis
Policy Manual (Version 1.0)

Effective Date: January 16, 2025

Releasability: Cleared for public release

Approved by: Ken Wainstein
Under Secretary for Intelligence and Analysis

Enclosures:

1. (U) I&A Lexicon
2. (U) References
3. (U) Abbreviations

Attachment: I&A Intelligence Oversight Guidelines

UNCLASSIFIED

Message From the Under Secretary for Intelligence and Analysis

I am proud to present the first Policy Manual for the Department of Homeland Security (DHS or the Department) Office of Intelligence and Analysis (I&A). Clear and accessible policy guidance is critical for any mature organization, but it is particularly essential for I&A. As a component of DHS and an element of the Intelligence Community, I&A must implement, and sometimes harmonize, direction from the Secretary of Homeland Security and the Director of National Intelligence. Further, I&A’s homeland security focus requires it to support a wide variety of missions while operating under significant legal and policy requirements and restrictions governing its intelligence activities. As a result, I&A personnel must have a clear, comprehensive understanding of the policies that set the parameters for their work.

Transparency is also integral to I&A’s sustained success. I&A cannot operate effectively without the trust and confidence of the American people. Whether through their elected representatives in Congress or directly, they deserve to know what I&A does and why it does it. By holding itself accountable through enhanced transparency, I&A ultimately will strengthen its ability both to deliver timely, actionable intelligence on homeland security threats and vulnerabilities to its federal, state, local, tribal, territorial, and private sector stakeholders, and protect privacy and civil liberties. For that reason, I&A is releasing the Policy Manual to the public.

The Policy Manual is intended to help I&A achieve these objectives. I&A developed the manual following a comprehensive “360 Review” of its internal organization, mission priorities, and functions over a two-year period. At the conclusion of that review, we determined that I&A’s policy documents should be updated and codified in a single document accessible to both the I&A workforce and the public. I therefore directed a comprehensive review of I&A’s existing policy instruments to ensure they are up to date, formatted in a manner that facilitates their use by the workforce, and accessible both to Congress and other external oversight entities, and subject to the need to protect sensitive sources and methods, to the public.

I&A exists to provide intelligence support to the Department and share information with federal, state, local, tribal, territorial, and private sector entities with homeland security responsibilities while upholding the principles of privacy, civil rights, and civil liberties. This Policy Manual enables that mission by ensuring better understanding of our governing policies both within I&A and by those outside I&A. I ask all I&A personnel to familiarize themselves with its contents, and I invite other readers to do the same.

Sincerely,



Kenneth L. Wainstein
Under Secretary for the Office of Intelligence and Analysis
U.S. Department of Homeland Security

General Guidance on the Policy Manual

The Policy Manual consolidates and codifies all unclassified organizational, programmatic, and administrative policies specific to I&A. It is organized by topic into five chapters reflecting I&A's organization and functions. Where necessary for readability, these chapters are further divided into subchapters. Each chapter or subchapter contains sections focusing on specific topics.

Adherence to Policy Guidance. All I&A personnel—meaning all I&A employees, including personnel temporarily assigned to act for I&A (i.e., detailees), and contractors supporting I&A—are required to familiarize themselves with, and follow, the policy guidance set forth in the Policy Manual. They are prohibited from engaging in any activity to avoid indirectly evading the policy guidance set forth in the Policy Manual, including by directing, demanding, or requesting any external entity to engage in conduct prohibited by policy guidance on their behalf. Adherence to the guidance set forth in this manual will be enforced through appropriate administrative actions.

I&A personnel are required to report any apparent, alleged, or suspected violations of the Policy Manual's policy guidance to their chain of command, OGC/ILD, or TOPO's Privacy and Intelligence Oversight Branch (TOPO/PIOB) for further action, as appropriate. Conduct reasonably believed to constitute a violation of federal law must be reported immediately to OGC/ILD or TOPO/PIOB, who will refer the matter immediately to OGC/ILD for further action.

Rules of Construction. The Policy Manual endeavors to use terms and titles consistently across its various parts and sections. Some terms and phrases used through the manual have specific meanings consistent with normal rules of construction. For example:

- The Policy Manual contains some terms that are defined by the policy guidance introducing them or in other authoritative DHS or I&A documents such as lexicons or I&A's Intelligence Oversight Guidelines. Terms not defined in this manner should be given their ordinary meaning.
- The Policy Manual uses the conjunctions “and” and “or” throughout the document when directing actions or imposing requirements. “And” is inclusive, meaning every action or requirement connected by the conjunction must be fulfilled. “Or” is exclusive, meaning any of the actions or requirements connected by the conjunction must be fulfilled.
- The Policy Manual uses the terms “shall,” “will,” “must,” and “should” to describe various actions to be undertaken. The first three terms indicate direction to undertake the activity; it would be a violation of I&A policy not to do so. The term “should” suggests a course of action. I&A personnel are encouraged and generally expected to pursue that course of action, but it will not violate I&A policy if they fail to do so.
- The Policy Manual sometimes refers to “coordination” or “consultation” with others when undertaking a course of action or producing a desired outcome (e.g., written work

product of some kind). These terms are not synonymous. “Coordination” means that the action or outcome in question must be approved by those providing the coordination. “Consultation” means those providing consultation must be allowed to review and provide feedback concerning the course of action or outcome before that course of action or outcome is completed.

- The Policy Manual uses the phrase “as appropriate” at various points as a caveat for directed or suggested actions. This phrase means that I&A will execute the directed or suggested action at their discretion provided their discretion is not exercised in an arbitrary manner. Instead, when acting “as appropriate,” I&A personnel are expected to exercise their discretion consistent with the underlying purposes and principles animating the directed or suggested action.
- The Policy Manual elaborates on its provisions at various points by stating that a provision includes one or more items (e.g., “This Policy Manual has many parts, including with respect to I&A’s analytic, collection, and partnership activities.”). Unless specified otherwise in the text, these items are illustrative, not exhaustive, of the broader or more general provisions they describe.
- The Policy Manual sometimes refers to specific authorities or policies. These references should be read as transferring to any successor authorities or policies, and responsibilities assigned to officials or organizations in the manual should be read as transferring to any successor official or organization exercising the relevant general responsibilities of the named official or organization.
- The Policy Manual often assigns specific responsibilities to designated officials. Unless otherwise specified in the text of the manual, these responsibilities may be carried out by subordinates to a designated official where directed, or appropriately delegated the authority, to do so.

The Policy and Coordination Oversight Branch within I&A’s Transparency and Oversight Program Office (TOPO/PCOB) is available to assist with questions regarding these and other rules of construction. Questions of interpretation for specific provisions of the Policy Manual should be referred to the Office of the General Counsel’s Intelligence Law Division (OGC/ILD).

Timeliness and Accuracy. The Policy Manual is intended to provide comprehensive, up-to-date, and accurate policy guidance to the I&A workforce. When I&A issues new or revised policy guidance, the content of that guidance will be incorporated in the Policy Manual, whether through a new part or section of the manual or through changes to existing parts or sections incorporating the new or revised policy guidance. I&A also will review and update the Policy Manual on a regular basis to ensure the offices, officials, and terms used throughout the manual are up to date and correct any technical errors in the manual.

Compliance With Law and Policy. The actions or outcomes directed or required by the Policy Manual are subject to the availability of appropriations and will be implemented and executed

consistent with the provisions of the Constitution, the laws of the United States, presidential guidance, regulation, and national, Intelligence Community, and departmental policy. If a provision within the Policy Manual is determined to be inconsistent with any of the authorities listed above, that provision will be inoperative, but the other provisions of the Policy Manual not subject to this inconsistency will remain in effect. Nothing in this manual creates, nor is anything in this manual intended to create, any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

TABLE OF CONTENTS

PART ONE: CROSS-ORGANIZATIONAL PROVISIONS

Subpart One: General Provisions

- 1-101 Mission
- 1-102 Organization of the Office of Intelligence and Analysis
- 1-103 Media Contacts and Speaking Engagements
- 1-104 Political Activities and Code of Ethics
- 1-105 Anti-Harassment and Anti-Discrimination
- 1-106 Executive Secretariat Task and Correspondence Management

Subpart Two: Transparency and Oversight

- 1-201 Intelligence Oversight Program
- 1-202 Reasonable Belief Statements
- 1-203 Information Systems and Bulk Data Holdings Audits
- 1-204 Safeguarding Personal Information Collected From Signals Intelligence Activities
- 1-205 Disclosure of Section 1367 Information
- 1-206 Special Handling Requirements for Congressional Identity Information
- 1-207 Privacy and Civil Liberties Oversight Program
- 1-208 Policy Coordination and Oversight
- 1-209 Internal Controls
- 1-210 Interactions With the U.S. Government Accountability Office
- 1-211 Protection of Sources and Methods Under the Freedom of Information Act
- 1-212 Organizational Ombuds
- 1-213 Whistleblower Protections

PART TWO: ANALYSIS

- 2-101 Organization of the Office of Analysis
- 2-102 Production of Finished Intelligence Products

PART THREE: COLLECTION

- 3-101 Organization of the Office of Collection
- 3-102 Open Source Intelligence Collection Program
- 3-103 Geospatial Reporting Program

PART FOUR: PARTNERSHIPS

Subpart One: General Provisions

- 4-101 Organization of the Office of Partnerships
- 4-102 Liaison Officer Program
- 4-103 Notification of Official Travel
- 4-104 Support to Requests for Information
- 4-105 State and Local Security Clearance Requests
- 4-106 Duty to Warn
- 4-107 Nationwide Functional Teams

Subpart Two: Field Intelligence

- 4-201 Field Intelligence Program
- 4-202 Engaging Partners in the Field
- 4-203 Use of Government Vehicles by Field Personnel

PART FIVE: MANAGEMENT

Subpart One: Operations

- 5-101 Organization of the Office of Management
- 5-102 Employee Recruitment, Selection, Conversion, and Promotion
- 5-103 Temporary Assignments, Extended Leave, and Management of Detailees
- 5-104 Leave, Premium Pay, Breaks, Alternative Work Schedules, Telework, and DHS Wellness Program
- 5-105 Employee Recognition and Awards
- 5-106 Planning, Programming, Budgeting, and Evaluation Program
- 5-107 Records and Information Management
- 5-108 Restrictions on Post-Government Employment

Subpart Two: Technology & Data Services

- 5-201 Planning, Procuring, and Managing Information Technology Resources
- 5-202 Responsible Framework for Use of Artificial Intelligence and Machine Learning
- 5-203 Use of Commercially Available Information

Subpart Three: Training

- 5-301 Career Development

UNCLASSIFIED

**PART ONE: CROSS-ORGANIZATIONAL
PROVISIONS**

UNCLASSIFIED

UNCLASSIFIED

1-101: Mission

The mission of the Office of Intelligence and Analysis (I&A)—to provide decisional advantage to homeland security leaders across the nation—arose from the 9/11 terrorist attacks. To fill the gaps in the nation’s homeland intelligence capabilities that were laid bare by those attacks, I&A has, from its inception, operated according to three guiding mandates: (1) to build and maintain an intelligence program within the United States that can detect and prevent threats to the homeland; (2) to serve as an information-sharing bridge between, on the one hand, Intelligence Community and federal law enforcement agencies, and departmental components; and, on the other hand, federal, state, local, tribal, territorial, and private sector (FSLTTP) partners; and (3) to operate with an intensely focused regard for privacy and civil liberties in recognition of the sensitivity around the conduct of intelligence activities within the United States.

(a) Intelligence Missions. In service of the broader mandates described above, I&A engages in intelligence activities encompassing the entire intelligence cycle, setting intelligence requirements; collecting (overtly or through publicly available sources) information responsive to those requirements for serialization in intelligence reports; and analyzing, producing, and disseminating analytic products. By statute and executive order, these activities are limited in scope to those that are reasonably believed to further a national or departmental mission of I&A.

(i) I&A personnel further a national mission where they assist the President or other executive branch officials performing executive functions in the development and conduct of foreign, defense, and economic policies or the protection of the United States national interests from foreign security threats, or, as appropriate, where they assist the Congress of the United States. Examples of foreign security threats include, but are not limited to—

- (A) International terrorism threats;
- (B) The proliferation of weapons of mass destruction;
- (C) Intelligence activities directed against the United States;
- (D) International criminal drug activities; and
- (E) Other hostile activities directed against the United States by foreign powers, organizations, persons, and their agents.

(ii) I&A personnel further a departmental mission where they assist DHS, other departments and agencies of the federal government, state and local government agencies and authorities, the private sector, or other entities in identifying protective and support measures regarding threats to homeland security, including, but not limited to—

- (A) Domestic terrorism threats;
- (B) Threats to critical infrastructure and key resources;
- (C) Significant threats to the nation’s economic security, public health, or public safety, including, but not limited to, local manifestations of national threats (e.g.,

UNCLASSIFIED

local outbreaks of diseases reasonably likely to pose the risk of becoming a national pandemic);

(D) Major disasters and other catastrophic acts; and

(E) Any other threat of such severity and magnitude that effective response would be beyond the capabilities of any affected state and local governments, such that federal assistance would be necessary.

In addition, the intelligence activities of I&A personnel further a departmental mission where they support the Secretary, the Deputy Secretary, the DHS Chief of Staff, or their respective staff, component heads, or any other departmental officials, offices, or elements in the execution of their lawful missions.

(b) Other Missions.

(i) In addition to the intelligence missions described in Section 1-101(a) above, I&A personnel support the Under Secretary for Intelligence and Analysis in the execution of their other intelligence-related responsibilities on behalf of the Department, including in support to state, local, and regional fusion centers and in their capacity as the Department's Chief Intelligence Officer; Counterintelligence Executive; Senior Information Sharing and Safeguarding Executive; Executive Agent for the Terrorist Watchlisting Process; Executive Agent for Intelligence, Surveillance, and Reconnaissance Capability; Official Responsible for Information Sharing; and co-chair of the Counter Threats Advisory Board.

(ii) These responsibilities fall outside the scope of this policy guidance and are addressed through separate policy channels and instruments applicable across the Department.

1-102: Organization of the Office of Intelligence and Analysis

The Office of Intelligence and Analysis (I&A) is a support (i.e., headquarters) component of the Department of Homeland Security (DHS) and an element of the Intelligence Community. It is led by the Under Secretary for Intelligence and Analysis (USIA), a presidentially appointed, Senate confirmed official who reports directly to the Secretary of Homeland Security (Secretary) and Deputy Under Secretary for Homeland Security when acting on behalf of the Secretary. The USIA also reports to the Director of National Intelligence as the head of the Intelligence Community. The USIA is the only political appointee at I&A.

The Principal Deputy Under Secretary for Intelligence and Analysis (PDUSIA) supports the USIA in the performance of all their responsibilities. This includes exercising the responsibilities of the USIA on the USIA's behalf and subject to their guidance, direction, and oversight. The PDUSIA is the senior career official within I&A. Both the USIA and PDUSIA are supported by the Chief of Staff and deputy undersecretaries responsible for the analysis, collection, partnerships, and management functions within I&A, respectively. This leadership structure is reflected in the organization and order of succession at I&A.

(a) Offices and Program Offices. I&A consists of five primary subcomponents, referred to as *offices*. These offices are as follows:

(i) *Front Office.* The Front Office provides immediate, direct support to the USIA and PDUSIA in the execution of their responsibilities. The USIA and PDUSIA lead the Front Office, and the Chief of Staff oversees its day-to-day activities.

(A) The functions performed by the Front Office include I&A's Executive Secretariat, communications specialists, and general staff support to the USIA and PDUSIA.

(B) The Front Office also contains two *program offices*: the Intelligence Enterprise Program Office (IEPO) and the Transparency and Oversight Program Office (TOPO). Program offices are small compared to offices, but they perform discrete functions that, by their nature, require dedicated Front Office attention. The heads of the program offices are senior executives who report directly to the USIA and PDUSIA concerning the execution of their functions.

(I) IEPO provides strategic and administrative support to the USIA in the USIA's role as Chief Intelligence Officer (CINT) for the Department and co-chair of the Counter Threats Advisory Board, supporting the CINT's coordination of the intelligence programs of other DHS components through the DHS Intelligence Enterprise and supporting intelligence policy development across DHS. IEPO also manages the DHS Counterintelligence Program, which focuses on protecting DHS and its personnel from adversarial intelligence activities. The program office is led by the Executive Director of IEPO (ED/IEPO).

(II) TOPO consolidates and elevates the transparency and oversight functions previously dispersed throughout I&A, with a special emphasis on ensuring that I&A conducts its mission with careful regard for privacy, civil rights, and civil liberties. The program office oversees the Privacy and Intelligence Oversight Branch, the Policy Coordination and Oversight Branch, the Internal Controls Branch, the Freedom of Information Act Branch, the Component Audit Liaisons, and the Organizational Ombuds. TOPO also provides support to congressional oversight of I&A through its executive team. The program office is led by the Director of TOPO (D/TOPO).

(ii) *Collection*. The Office of Collection oversees I&A's collection of information about homeland security threats and vulnerabilities, preparing and disseminating serialized intelligence reports to I&A's partners. The office guides I&A's collection activities, which focus on liaison and open source collection. It also oversees I&A's identities intelligence activities in support of the Department's screening and vetting efforts. The Office of Collection manages collection requirements and implements compliance measures to ensure that personnel have adequate training and resources to execute their operations in accordance with policy guidance and the direction of leadership. The office is led by the Deputy Under Secretary for Collection (DUS/C).

(iii) *Analysis*. The Office of Analysis produces primarily strategic intelligence products for DHS stakeholders, including senior government officials, federal partners, and state, local, tribal, territorial, and private sector professionals. Its four analytic centers—the Counterterrorism Center, the Nation-State Threat Center, the Cyber Intelligence Center, and the Transborder Security Center—serve as the Department's centers of gravity for the analysis of the most critical threats to the homeland. The office is led by the Deputy Under Secretary for Analysis (DUS/A).

(iv) *Partnerships*. The Office of Partnerships coordinates I&A's federal, state, local, tribal, territorial, private sector, and foreign partner relationships, fosters an intelligence network among those partners, and oversees I&A's intelligence officers deployed around the country. The office also oversees I&A's Intelligence Watch and Coordination Center, which provides 24/7 situational awareness to DHS leaders and produces updates on emerging events, I&A's Request for Information Program, and the Department's Special Events Program. The office is led by the Deputy Under Secretary for Partnerships (DUS/P).

(v) *Management*. The Office of Management provides the administrative support that enables I&A's mission, including technology and data services, financial management, training, recruiting, human resources, security, and facilities management. The office is led by the Deputy Under Secretary for Management (DUS/M).

Collectively, the heads of the offices and program offices described above comprise the I&A Senior Staff.

(b) Organizational Units Within Offices and Program Offices. I&A's offices and program offices are further subdivided into *directorates*, *centers*, *divisions*, and *branches*.

(i) *Directorates* are the next level of organizational unit down from an office. Generally, they have a broader range of responsibilities than centers or divisions. Directorates include branches within them, and some directorates are large enough that they include divisions. They are led by directors, who are senior executives who report directly to their cognizant office heads.

(ii) *Centers* are organizational units within an office that engage in analytic or identities intelligence activities. In terms of organizational level, they are equivalent to divisions and subordinate to directorates; currently, there are no centers within directorates. Centers include branches within them. They are led by directors, who are senior executives who report directly to their cognizant office heads.

(iii) *Divisions* are organizational units within an office or directorate. In terms of organizational level, they are equivalent to centers, but do not perform the functions of centers. Divisions include branches within them. They are led by directors, who are senior executives who report directly to their cognizant office or directorate heads.

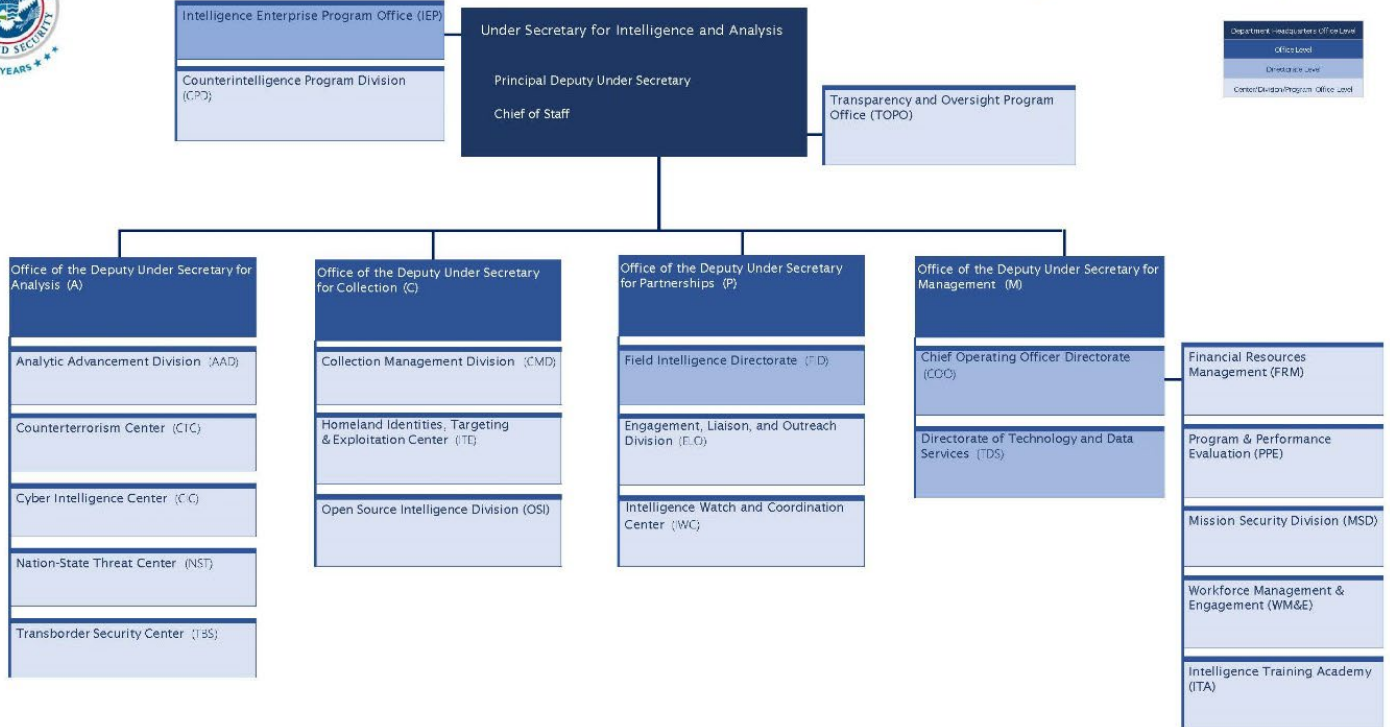
(iv) *Branches* are organizational units within program offices, centers, and divisions (and directorates for those lacking divisions within them). They vary in size and function. Branches are led by chiefs, who occupy supervisory billets and report directly to their cognizant program office, directorate, center, or division head.

The specific directorates, centers, divisions, and branches within each office are described in the policy guidance explaining the organization of those offices.

The chart below presents the current organization of I&A.



Office of Intelligence and Analysis



1-103: Media Contacts and Speaking Engagements

Office of Intelligence & Analysis (I&A) personnel are responsible for protecting intelligence sources, methods, and activities from unauthorized disclosure, preserving privileged information, protecting the rights of individuals, and complying with applicable law and policy. Personnel who fail to comply with laws and policies that protect against the unauthorized disclosure of official information or misuse of appropriated funds may be subject to administrative, civil, and criminal penalties.

The Under Secretary for Intelligence and Analysis (USIA), as the designated spokesperson for I&A, is committed to sharing information responsibly with the public to further government transparency and enhance public understanding of I&A's mission, the laws and authorities that govern our activities, and our compliance and oversight framework. Responses to the media are tempered by considerations for the potential impact on public safety, ongoing criminal or civil investigations, sensitive foreign activities, pre-decisional matters, operational factors, the exchange of intelligence, and matters in litigation. Substantive information concerning sensitive intelligence-related information, including information about sensitive intelligence sources, methods, activities, or judgments is never provided to the media.

(a) Engaging With the Media. In coordination with the Department of Homeland Security (DHS) Office of Public Affairs (OPA) and the Office of the Director of National Intelligence Public Affairs Office (ODNI/PAO), and except as provided in Section 1-103(a)(i) below, the USIA delegates authority to I&A personnel to engage with the media on a case-by-case basis. Authorization for a particular contact does not constitute authorization for additional media engagement.

(i) The Principal Deputy Under Secretary for Intelligence and Analysis (PDUSIA), Chief of Staff, and the I&A Senior Communications Specialist may engage with the media on the USIA's behalf.

(ii) All matters regarding media contact, speaking engagements, and public speaking opportunities must be coordinated with the PDUSIA, Chief of Staff, or Senior Communications Specialist. The PDUSIA, Chief of Staff, or Senior Communications Specialist approve requests on behalf of the USIA, as appropriate.

(iii) The Senior Communications Specialist consults with OPA and ODNI/POA on matters regarding media contact, as appropriate. Consultation with ODNI/POA is required when media contact involves support to projects such as books, television programs, documentaries, motion pictures, and similar works related to sensitive intelligence sources, methods, activities, and judgments.

(b) Unintentional Contact With the Media. If I&A personnel receive an inquiry from an individual reasonably believed to be a member of the media regarding a DHS or intelligence matter, those personnel must—

(i) Direct inquiries to OPA;

- (ii) Notify the Senior Communications Specialist of the media contact; and
 - (iii) Take further action only as instructed by the Senior Communications Specialist.
- (c) Reporting Contact With the Media. The Senior Communications Specialist reports semi-annually to ODNI/PAO on I&A's media contacts, including—
- (i) The names or positions of I&A personnel designated in writing to have contact with the media;
 - (ii) The names or positions of I&A personnel who have been delegated by the USIA on a case-by-case basis to have contact with the media and the matters on which they were authorized to have contact; and
 - (iii) Any substantive contact with the media that were unintentional or unplanned and the topic of discussion.
- (d) Speaking Engagements. I&A personnel interested in participating in a speaking engagement, or recommending I&A senior leadership for a speaking engagement, are required to fill out the DHS Speakers Request Form located at <https://www.dhs.gov>. Speaking engagements include, but are not limited to, conferences, panels, webinars, interviews, media, and podcasts.
- (i) Prior to accepting any engagements, personnel must submit the DHS Speakers Request form to the Senior Communications Specialist. The Senior Communications Specialist submits the approved request to the DHS Office of the General Counsel (OGC) for review.
 - (ii) After OGC clearance, the Senior Communications Specialist submits the completed form and any corresponding attachments to the DHS Speakers Bureau.
 - (iii) Even if I&A personnel are asked to speak in a personal capacity, they must provide information to their supervisor and the Senior Communications Specialist for review and clearance by OGC.
 - (A) Any offers of reimbursement or travel must be cleared by OGC.
 - (B) DHS personnel are prohibited from signing non-DHS release/disclaimer forms.
- DHS Directive No. 110-02, *Public Speaking Opportunities* (Apr. 11, 2019), contains further guidance for the coordination and approval of public speaking invitations by DHS employees.
- (e) Violations. The Senior Communications Specialist, through the Chief of Staff, refers reports of unauthorized media contacts by I&A personnel to the DHS Office of Public Affairs and the DHS Office of the Chief Security Officer, as appropriate.

1-104: Political Activities and Code of Ethics

The political activities of Office of Intelligence and Analysis (I&A) personnel, like other federal employees, are subject to provisions within the Hatch Act of 1939. Those restrictions are intended to maintain a federal workforce that is free from partisan political influence or coercion while allowing government personnel to participate in the political process.

(a) Political Activities.

(i) “Political activity” includes any activity directed toward the success or failure of a political party or a candidate for a partisan political office.

(ii) Most employees are permitted to engage in a wide range of partisan political activities during off-duty hours, but may not engage in political activities while on duty.

(iii) I&A personnel are encouraged to contact the Office of the General Counsel’s Intelligence Law Division (OGC/ILD) for specific guidance regarding limitations on political activities.

(b) Code of Ethics. I&A follows Department of Homeland Security (DHS) policy on the distribution and acceptance of gifts by personnel.

(i) Per DHS Directive No. 112-02, *Gifts to the Department of Homeland Security* (Feb. 11, 2008), DHS Instruction No. 112-02-01, *Instruction Guide on Gifts to the Department of Homeland Security* (Feb. 12, 2008), and DHS Delegation No. 00006, *Delegation to Accept and Utilize Gifts to the Department* (as amended Feb. 26, 2019), no employee of DHS may solicit gifts or encourage the solicitation of gifts to DHS unless the Secretary of Homeland Security, Deputy Secretary of Homeland Security, or an authorized agency official approves the solicitation in advance. The solicitation or acceptance of a gift must not compromise the integrity of DHS, its programs, operations, or employees.

(ii) Each I&A employee must respect and adhere to the principles of ethical conduct set forth in 5 C.F.R. Part 2635, *Standards of Ethical Conduct for Employees of the Executive Branch*, DHS Directive No. 0480.1, *Ethics/Standards of Conduct* (March 1, 2003), and the applicable laws of the United States. Per DHS Directive No. 0480.1, all employees will maintain especially high standards of honesty, impartiality, character, and conduct to ensure the proper performance of government business and the continual trust and confidence of the citizens of the United States.

(A) The conduct of employees must reflect the qualities of courtesy, integrity, and loyalty to the United States; a deep sense of responsibility for the public trust; promptness in dealing with and serving the public; and a standard of personal behavior that reflects positively on and will be a credit to both employees and DHS.

(B) These principals apply to official conduct as well as private conduct that affect in any way the ability of employees or DHS to effectively accomplish the work of DHS.

(iii) Per DHS Directive No. 4600.1, *Personal Use of Government Office Equipment* (Apr. 14, 2003), DHS employees may use government office equipment for authorized purposes only. As set forth within DHS Directive No. 4600.1, limited personal use of the government office equipment by employees during non-work time is considered an “authorized use” of Government property where such use—

- (A) Involves minimal additional expense to the government;
- (B) Is performed on the employee’s non-work time;
- (C) Does not reduce productivity or interfere with the mission or operations of DHS organizational elements; and
- (D) Does not violate the Standards of Ethical Conduct for Employees of the Executive Branch.

1-105: Anti-Harassment and Anti-Discrimination

The Office of Intelligence and Analysis (I&A) is committed to fostering a culture of trust, respect, and integrity. As an organization, we all work together to cultivate an atmosphere that is free from harassment, discrimination, and retaliation.

(a) Anti-Harassment.

(i) Department of Homeland Security (DHS) Directive No. 256-01, *Anti-Harassment Program* (as amended May 24, 2019), and DHS Instruction No. 256-01-001, *Anti-Harassment Program* (June 7, 2019), set forth the Department's anti-harassment procedures and established requirements for preventing workplace harassment and addressing and resolving allegations of harassment within DHS's civilian workforce. As a component of DHS, I&A refers to this guidance for anti-harassment matters and collaborates with the DHS Anti-Harassment Unit in carrying out the procedures outlined therein.

(ii) Harassment is prohibited at DHS and will not be tolerated in any form. DHS prohibits harassment even if it does not rise to a level that violates the law. Although a single harassing utterance or act may not rise to a level that is actionable under the law, it still has no place at DHS and may be considered misconduct under DHS policy.

(iii) DHS anti-harassment policy prohibits harassment by any DHS employee, or harassment of any DHS employee or applicant, by any employee, contractor, vendor, applicant, or other individual with whom DHS employees come into contact by virtue of their work for DHS.

(iv) All employees must report harassing conduct they have witnessed in accordance with applicable reporting procedures.

(v) More information on DHS's anti-harassment policy is available at DHS Directive No. 256-01, DHS Instruction No. 256-01-001, and DHS Policy Statement No. 256-06, *DHS Anti-Harassment Policy Statement* (as amended July 2, 2024).

(b) Equal Employment Opportunity and Anti-Discrimination. Equal employment opportunity (EEO) is the right to obtain employment and advance professionally on the bases of merit, ability, and potential in a work environment free from prejudice and discrimination.

(i) Consistent with EEO principles, employment discrimination based on race, color, religion, sex (including sexual orientation, gender identity, gender expression, and pregnancy), national origin, age, disability (including an individual's need for workplace reasonable accommodations), protected genetic information, parental status, and reprisal for prior protected EEO activities is prohibited at I&A. These protections extend to all management practices and decisions, including recruitment and hiring practices, appraisal systems, promotions, training, and career development programs.

(ii) More information on DHS's EEO policies is available at DHS Policy Statement No. 256-08, *Equal Employment Opportunity and Anti-Discrimination Statement* (as amended Oct. 11, 2022).

1-106: Executive Secretariat Task and Correspondence Management

The Office of Intelligence and Analysis (I&A) Executive Secretariat (Exec Sec), led by the Executive Secretary, provides the Under Secretary for Intelligence and Analysis (USIA) with a responsive, efficient, and collaborative process for task and correspondence management. Exec Sec speaks on behalf of the USIA, Principal Deputy Under Secretary for Intelligence and Analysis (PDUSIA), and Chief of Staff on all internal and external tasking matters. Exec Sec's experienced team of analysts ensures that tasks are completed to the highest standards of quality and professionalism and shared appropriately with stakeholders.

I&A manages official tasks and executive correspondence through Exec Sec, using uniform and coordinated procedures according to the Department of Homeland Security (DHS) Executive Correspondence Handbook. The Executive Secretary is the only I&A official besides the USIA, PDUSIA, or Chief of Staff who may reject an official task for I&A and communicate such decision to the external requestor.

(a) Task Management Procedures.

(i) Task management commences when I&A receives an official task from an external entity or the USIA, PDUSIA, or Chief of Staff.

(A) Exec Sec assesses, in consultation with I&A Senior Leadership, as appropriate, whether the task is appropriately assigned to I&A, and if so, assigns a lead office.

(B) If a directorate, center, division, or branch receives an Official Task from an external entity directly, it must forward the task through established internal channels to Exec Sec for formal tasking. However, the recipient should immediately begin working the task and not reject it. If the recipient believes the task is not appropriate, it states such to Exec Sec, which determines whether to reject the task and communicate such decision to the external entity.

(ii) Exec Sec logs the task into the Correspondence Analyst Tracking Tool (CATT) system (or approved successor system) and assigns tracking numbers, determines task leads and required coordinators, sets internal timelines, and establishes formatting and other requirements.

(iii) Exec Sec reviews the draft task response for completeness, consistency, accuracy, style, tone, formatting, and grammar.

(iv) Exec Sec determines which other internal or external entities are required to review and clear the draft task response and obtains clearance of the draft response from those entities, tracking the clearance process and maintaining a record of clearances and version control in CATT.

(v) The Chief of Staff determines if the task response must receive final approval from the USIA or PDUSIA. Exec Sec obtains the appropriate final approval.

(vi) Exec Sec submits, disseminates, and maintains an archive copy of all final task responses in accordance with departmental records management procedures using CATT.

(vii) If task requestors provide any feedback on I&A task responses, Exec Sec ensures such information is provided to the appropriate entities within I&A. Exec Sec maintains this information with the archived task documents.

(b) Correspondence Management Procedures.

(i) Exec Sec sets all formatting and style guidelines for I&A Executive Correspondence consistent with the DHS Executive Correspondence Handbook and guidance from the USIA, PDUSIA, or Chief of Staff.

(ii) Personnel use approved templates for I&A executive correspondence. Exec Sec ensures that all approved templates are maintained in a document repository available on both I&A Connect and in the I&A Library on the I&A Shared Drive. Exec Sec updates all templates as necessary.

(iii) Personnel seeking to obtain signature from the USIA, PDUSIA, or Chief of Staff on correspondence or other documents submit the correspondence or documents to Exec Sec.

(iv) Personnel seeking decision or signature from the Secretary of Homeland Security (Secretary) or Deputy Secretary of Homeland Security (Deputy Secretary) on correspondence or documents submit the correspondence or documents to Exec Sec with a DHS cover memorandum per the DHS Executive Correspondence Handbook. Information memoranda (not seeking decision or signature) for the Secretary or Deputy Secretary do not require a DHS cover memorandum.

(v) For correspondence or documents prepared in response to Exec Sec tasks, personnel need only provide the accompanying documents that Exec Sec specifies in the task (i.e., if a cover memorandum is not requested in the task, it is not required for the response).

(vi) Internal correspondence and documents receiving final clearance and signature by a Deputy Under Secretary or equivalent are managed by the respective lead office and need not be provided to I&A Exec Sec. These correspondence and documents may, however, be provided to external entities for clearance, as appropriate, and the correspondence and documents should conform to all formatting and style guidance provided by DHS and I&A Exec Sec to ensure consistency and quality of all I&A correspondence.

1-201: Intelligence Oversight Program

As an Intelligence Community element with a homeland-focused mission, the Office of Intelligence and Analysis (I&A) has an acute obligation to protect the rights of the American people. Consequently, I&A must always operate with an intensely focused regard for privacy, civil rights, and civil liberties—a mission on par with its missions to provide intelligence support to the Department and share information with federal, state, local, tribal, territorial, and private sector entities with homeland security responsibilities.

The Intelligence Oversight Program is critical to I&A’s continued fidelity to these obligations. It provides the training, resources, and compliance work necessary for I&A personnel to understand and follow the privacy, civil rights, and civil liberties safeguards that apply to their work. And it provides transparency both within and outside I&A concerning the conduct of I&A’s intelligence activities so I&A can maximize its protection of privacy, civil rights, and civil liberties, including by being held accountable for its actions. This work focuses primarily on understanding and adhering to the requirements of I&A’s Intelligence Oversight Guidelines and their Implementation Guidance.

The Intelligence Oversight Guidelines and their Implementation Guidance provide foundational direction to I&A personnel on the conduct of their intelligence activities from a legal, privacy, civil rights, and civil liberties perspective. The Intelligence Oversight Guidelines are attached to this Policy Manual and available separately to the public online. Compliance with the Intelligence Oversight Guidelines and their Implementation Guidance satisfies the requirement in § 2.3 of Executive Order No. 12,333, *United States Intelligence Activities* (as amended July 30, 2008), that I&A collect, retain, and disseminate information about U.S. persons only in accordance with procedures established by the head of the Intelligence Community element concerned or by the head of a department containing such an element, and approved by the Attorney General following consultation with the Director of National Intelligence.

1-201-01. Fundamental Concepts of Intelligence Oversight.

(a) Meaning of Intelligence Oversight. Intelligence oversight refers to efforts within the Office of Intelligence and Analysis (I&A) to ensure its intelligence activities comply with requirements, restrictions, and protections to safeguard individuals’ privacy, civil rights, and civil liberties as distilled and codified in I&A’s Intelligence Oversight Guidelines and their Implementation Guidance.

(i) Other privacy, civil rights, and civil liberties safeguards (regardless of origin) that apply to I&A personnel are addressed through I&A’s Privacy and Civil Liberties Program, which is administered separately by the Privacy and Intelligence Oversight Branch within I&A’s Transparency and Oversight Program Office (TOPO/PIOB).

(ii) I&A’s obligations to comply with the rules, requirements, and restrictions set forth in the Intelligence Oversight Guidelines and their Implementation Guidance are referred to collectively as “intelligence oversight obligations” throughout this guidance.

(b) Expectations for Conduct. At all times, I&A personnel must maintain the highest standard of professional and personal conduct when engaging in the performance of their official duties, including by fulfilling the training requirements set forth in Section 1-201-03(b)(1) below.

(i) They are authorized to act only in accordance with the Constitution; the laws of the United States; executive orders and other presidential, interagency, Intelligence Community, the Department of Homeland Security (DHS), and I&A guidance, regardless of the form in which it is communicated; and international and domestic agreements, arrangements, and obligations.

(ii) This includes, but is not limited to, intelligence oversight obligations, and includes all applicable legal, regulatory, policy, and other binding requirements on I&A personnel.

(c) Reporting Obligations. I&A personnel are required to report any apparent, alleged, or suspected violations of any of the expectations for conduct set forth in Section 1-201-01(b) above, including, but not limited to intelligence oversight obligations, to either TOPO/PIOB or the Office of the General Counsel's Intelligence Law Division (OGC/ILD), and preferably to both. The apparent, alleged, or suspected violation should be reported as soon as possible, but in any event not later than 24 hours after becoming aware of the potential violation.

(i) Any apparent, alleged, or suspected violation of an intelligence oversight obligation (otherwise known as a "questionable intelligence activity (QIA)") reported to TOPO/PIOB will be addressed consistent with the processes governing compliance inquiries as described in Section 1-201-03(c)(i)(A) below unless the QIA concerns a significant or highly sensitive matter.

(A) A significant or highly sensitive matter is any intelligence activity (regardless of whether the intelligence activity is unlawful or contrary to executive order or presidential directive) or serious criminal activity by I&A personnel that could be expected to impugn the reputation or integrity of the Intelligence Community or otherwise call into question the propriety of intelligence activities, as defined by the PIOB's Concept of Operations. A "significant or highly sensitive matter" is not necessarily limited to violations of I&A's Intelligence Oversight Guidelines.

(B) TOPO/PIOB will refer any QIA constituting a significant or highly sensitive matter to OGC/ILD immediately for further action, as appropriate. TOPO/PIOB will consult with OGC/ILD to determine whether to resume its processes governing compliance inquiries as described in Section 1-201-03(c)(i)(A) below.

(ii) Any apparent, alleged, or suspected violation of an expectation for conduct by I&A personnel that is reported to TOPO/PIOB, but not to OGC/ILD, and is not a QIA will be referred to OGC/ILD as soon as is practicable unless it concerns a significant or highly sensitive matter, in which case it will be referred to OGC/ILD immediately.

1-201-02. Purpose and Scope of the Intelligence Oversight Program. The Intelligence Oversight Program exists to facilitate workforce understanding of, and compliance with, intelligence oversight obligations.

(a) Types of Conduct Within the Program's Scope. The Intelligence Oversight Program focuses on intelligence oversight obligations. Expectations for conduct not related to those activities, such as compliance with human capital, information technology, security, or budgetary requirements or restrictions, are not within its scope.

(b) Intelligence Activities Within the Program's Scope. The Intelligence Oversight Program focuses on the intelligence activities of I&A. Intelligence activities of other DHS components, offices, or elements, or personnel therein, are not within the scope of the program unless they are being carried out for or on behalf of I&A or pursuant to authorities to conduct intelligence activities delegated by the Under Secretary for Intelligence and Analysis (USIA).

1-201-03. Functions of the Intelligence Oversight Program. There are three primary functions of the Intelligence Oversight Program, which are addressed in turn below.

(a) Workforce Guidance and Materials. The Intelligence Oversight Program assists I&A personnel in implementing intelligence oversight protections in specific contexts, whether through formal guidance memoranda, reference or pedagogical materials, or informal consultations or reviews of I&A proposals, initiatives, or work product.

(i) Guidance provided by the Intelligence Oversight Program is limited to the implementation of intelligence oversight obligations. The interpretation of the scope, meaning, and applicability of these obligations is reserved to OGC/ILD.

(ii) Accordingly, any issues presented to the Intelligence Oversight Program giving rise to novel or unusually complex questions of interpretation of intelligence oversight protections are coordinated with, or referred to, OGC/ILD, as appropriate.

(b) Training. The Intelligence Oversight Program provides comprehensive training to I&A personnel on intelligence oversight protections.

(i) I&A personnel, including individuals detailed to I&A and contract support, are required to complete this training not later than 30 days after commencing employment, their detail, or contract support, and at least annually thereafter. I&A personnel are not permitted to engage in any intelligence activity subject to intelligence oversight obligations without first completing intelligence oversight training.

(ii) The Deputy Under Secretary for Management (DUS/M), acting through the Director of the Intelligence Training Academy (D/ITA), supports the development and delivery of this training.

(c) Compliance. The Intelligence Oversight Program engages in compliance activities on a regular basis to identify, address, and recommend measures to mitigate any failures by I&A personnel to comply with intelligence oversight protections.

(i) *Compliance Mechanisms*. The Intelligence Oversight Program uses three mechanisms to assess compliance with intelligence oversight protections: compliance inquiries, compliance audits, and compliance reviews.

(A) Compliance inquiries are *ad hoc* administrative fact-finding processes to determine whether a reported QIA constitutes a violation of an intelligence oversight obligation.

(B) Compliance audits are scheduled administrative fact-finding processes that are conducted to fulfill a specific auditing requirement imposed by law, regulation, policy, or some other binding authority, including, but not limited to, the Intelligence Oversight Guidelines.

(I) Unlike compliance inquiries, compliance audits are not focused on specific QIAs. Rather, they assess I&A intelligence activities; functions; initiatives; programs, analytic products or intelligence reports; or access to, and use of, systems or data holdings (including, but not limited to, bulk data holdings) over a defined period to assess their compliance with intelligence oversight obligations.

(II) The Intelligence Oversight Program conducts compliance audits in response to, and consistent with, any binding deadlines imposed on the program. Where no specific deadline is imposed, the program will endeavor to complete the audit within one year of the receipt of the requirement. For ongoing audit requirements with no specified periodicity, the program will endeavor to conduct the required audit on a regular basis consistent with the availability of resources and considering competing priorities such as ongoing compliance inquiries.

(III) In any event, the Intelligence Oversight Program will complete at least one compliance audit each fiscal year.

(C) Compliance reviews are scheduled, proactive administrative fact-finding processes initiated by the Intelligence Oversight Program that are conducted to assess I&A intelligence activities; functions; programs; operations; initiatives; capabilities; work product (e.g., analytic products or intelligence reports); or access to, and use of, systems or data holdings (including, but not limited to, bulk data holdings) over a defined period to assess their compliance with intelligence oversight requirements.

(I) Unlike compliance inquiries, compliance reviews are not focused on specific QIAs. Unlike compliance audits, compliance reviews are not required by law, regulation, policy, or some other binding authority, but rather are initiated at the discretion of the Privacy and Intelligence Oversight Officer.

(II) The Intelligence Oversight Program conducts compliance reviews on a semiannual basis consistent with schedules approved by the USIA and the availability of resources, and considering competing priorities such as ongoing compliance inquiries and required compliance audits.

(III) In any event, the Intelligence Oversight Program will conduct at least one compliance review each fiscal year.

(D) In addition to formal, scheduled compliance inquiries, audits, and reviews, the Intelligence Oversight Program may conduct unannounced reviews (i.e., “spot checks” or “inspections”), including, but not limited to reviews of audit logs, records reviews, or informal employee or contractor interviews at any time at its discretion. Any QIAs arising from an unannounced review will be processed as compliance inquiries in accordance with Section 1-201-03(c)(ii) below.

(ii) *Compliance Processes.* The processes used for the different compliance mechanisms described in Section 1-201-03(c)(i) above vary from one mechanism to the next; accordingly, these processes will be memorialized in standard operating procedures issued by the D/TOPO in consultation with the DUS/M and the Deputy Under Secretaries for Analysis, Collection, and Partnerships, and the Executive Director of the Intelligence Enterprise Program Office. Nevertheless, the processes share certain features, which are described below.

(A) For each compliance mechanism, the Privacy and Intelligence Oversight Officer develops factual findings and compliance determinations regarding the subject of the compliance inquiry, audit, or review. The D/TOPO reviews these findings and determinations and, as appropriate based on the findings and determinations and in consultation with the heads of any affected subcomponents, recommends measures to mitigate any potential future violations of intelligence oversight requirements.

(B) The factual findings, compliance determinations, and any mitigation recommendations are submitted to the USIA and PDUSIA for awareness and decision regarding the mitigation recommendations. They are also provided to the Associate General Counsel for Intelligence (AGC/Intel) to inform a determination as to whether further referral of the information contained in the findings and determinations is appropriate.

(C) The Intelligence Oversight Program will notify the head of any subcomponent subject to a formal compliance inquiry, audit, or review or informal compliance activity before conducting such inquiry, audit, review, or activity except where prior notice reasonably could be expected to compromise the integrity or utility of the inquiry, audit, review, or activity, in which case notice will be provided as soon as possible during or after the conclusion of the inquiry, audit, review, or activity.

(D) I&A personnel will support any formal compliance inquiries, audits, reviews, or informal compliance activities to the maximum extent possible.

1-201-04. Administration of the Intelligence Oversight Program. The functions of the Intelligence Oversight Program are performed by the Privacy and Intelligence Oversight Officer and TOPO/PIOB subject to the guidance, direction, and oversight of the D/TOPO.

(a) The D/TOPO is the designated Senior Privacy and Civil Liberties Officer for I&A pursuant to ICD 107. In that capacity, they serve as the primary point of contact with I&A and departmental leadership regarding privacy, civil rights, and civil liberties policy and the senior I&A representative at departmental, Intelligence Community, and interagency meetings or fora on privacy, civil rights, and civil liberties matters. They also provide overall guidance, direction, and oversight concerning the activities of the Intelligence Oversight Program through the Privacy and Intelligence Oversight Officer.

(b) The Privacy and Intelligence Oversight Officer is responsible for the day-to-day activities of the Intelligence Oversight Program. In that capacity, they advise the D/TOPO and, as appropriate, I&A and departmental leadership regarding privacy, civil rights, and civil liberties policy and represent I&A at departmental, Intelligence Community, and interagency meetings or fora on privacy, civil rights, and civil liberties matters. They also complete compliance inquiries, audits, and reviews with the support of TOPO/PIOB staff.

(i) To ensure the objectivity and integrity of the Intelligence Oversight Program, the D/TOPO will facilitate, encourage, and refrain from impeding the Privacy and Intelligence Oversight Officer's communications on any matter pertaining to a reported potential violation of an intelligence oversight requirement, whether with the D/TOPO or separately, with the USIA, Principal Deputy Under Secretary for Intelligence and Analysis, AGC/Intel, Chief Privacy Officer, or Officer for Civil Rights and Civil Liberties.

(ii) The D/TOPO shall not mandate any revision to factual findings or compliance determinations made by the Privacy and Intelligence Oversight Officer arising from a compliance inquiry, audit, or review; however, they may suggest revisions or provide feedback thereto when requested by the Privacy and Intelligence Oversight Officer.

1-201-05. Transparency. To the maximum extent possible consistent with the protection of sources and methods, any applicable privileges, and other bases for withholding information under the Freedom of Information Act (FOIA) with respect to disclosure to the public, I&A will notify the Chief Privacy Officer, the Officer for Civil Rights and Civil Liberties, and Congress of any factual findings and compliance determinations arising from a compliance inquiry, audit, or review along with any actions directed by the USIA in response to those findings and determinations and post a copy of those artifacts in I&A's FOIA Reading Room.

1-201-06. Access to Information.

(a) Provision of Access to Offices of Inspectors General. Through the Component Audit Liaison (CAL), I&A personnel, without delay, will provide access to any information in its possession to the Office of the DHS Inspector General or the Office of the Inspector General of the Intelligence Community in response to any request for information where the requesting office deems such information necessary to perform its official duties, provided that any staff within these entities requesting such information possess the clearances and access to secure facilities necessary to acquire or review the information. The CAL will consult with OGC/ILD on the provision of access to these entities, as appropriate.

(b) Provision of Access to Other Oversight Offices. I&A personnel, without delay, will provide access to any information in its possession to OGC (including, but not limited to, OGC/ILD); the DHS Privacy Office; the DHS Office for Civil Rights and Civil Liberties; or TOPO/PIOB in response to any request for such information where the requesting office deems such information necessary to perform its official duties.

1-202: Reasonable Belief Statements

I&A's Intelligence Oversight Guidelines provide a comprehensive set of rules and procedures governing I&A's intelligence activities. At the same time, they are necessarily general given the scope of I&A's intelligence activities. They were never meant to provide instructions on the application of those rules and procedures to specific contexts. More recently, I&A issued Implementation Guidance for the Intelligence Oversight Guidelines to address some of the most pressing intelligence oversight topics of interest to I&A personnel. The Implementation Guidance's contents are authoritative, and all I&A personnel are expected to understand and follow them.

One way I&A has helped ensure compliance with this requirement is through the use in some circumstances of "Reasonable Belief Statements" that explain how reporting furthers a national or departmental mission. To further strengthen I&A's protection of privacy, civil rights, and civil liberties, we will expand this best practice in two ways. First, Reasonable Belief Statements explaining how reporting furthers a national or departmental will be required for all analytic products, serialized intelligence reports (e.g., Intelligence Information Reports, Field Intelligence Reports, and Open Source Intelligence Reports), or other materials intended for, or reasonably likely to be, disseminated outside I&A (collectively referred to throughout as "covered materials").¹ Second, additional information will be required for Reasonable Belief Statements falling within one or more of the categories described in Section 2(c) below consistent with that guidance.² These requirements will take effect on a rolling basis as I&A develops the capabilities to create and maintain these statements without placing undue logistical or administrative burdens on the I&A personnel charged with developing them.

(a) Purpose and Use. Reasonable Belief Statements are important tools that enable I&A personnel to articulate the reasonable bases and rationale for the covered materials they produce, ensuring a better understanding of how I&A's intelligence activities further national and departmental missions. They do not need to be shared with the recipients of their corresponding covered materials.

(b) Support for the Development of Reasonable Belief Statements. The creation of Reasonable Belief Statements should not distract I&A personnel from the conduct of their intelligence functions. The statements are meant to clarify, supplement, and contextualize intelligence activities, not chill or frustrate them.

¹ This would include materials created for internal use that are reasonably likely to be incorporated in other materials likely to be disseminated outside I&A such as curated lists or trackers that inform analytic products.

² The required contents of Reasonable Belief Statements vary according to the different missions described below, which match the national and departmental missions listed in I&A's Intelligence Oversight Guidelines as further described in their Implementation Guidance. The list below is intended solely to provide safeguards in the event I&A engages in intelligence activities in support of any of the listed missions and should not be interpreted as directing I&A personnel to pursue those missions. The prioritization of I&A's intelligence activities is addressed through I&A's Program of Analysis and Operating Directive.

(i) To reduce the logistical and administrative burdens on I&A personnel producing covered materials, the Director of the Transparency and Oversight Program Office (D/TOPO) will work with the Deputy Under Secretary for Analysis (DUS/A), the Deputy Under Secretary for Partnerships (DUS/P), the Deputy Under Secretary for Collection (DUS/C), and the Executive Director of the Intelligence Enterprise Oversight Program Office (ED/IEPO) to develop (or update existing) user-friendly templates that reduce the need for manual entries and recordkeeping of Reasonable Belief Statements by I&A personnel to the greatest extent possible.

(ii) The Deputy Under Secretary for Management (DUS/M), through the Director of the Technical and Data Services Directorate (D/TDS), will provide technical support to the development and deployment of these user-friendly templates consistent with current technical capabilities and available resources.

(iii) I&A personnel will begin to create Reasonable Belief Statements on a rolling basis as the user-friendly templates developed (or updated) to facilitate them are deployed.

(c) Required Contents.

(i) All Reasonable Belief Statements will explain the national or departmental mission(s) furthered by the covered material and the reason I&A personnel believe the covered material furthers that mission (or those missions).

(ii) Reasonable Belief Statements will also include the following:

(A) For covered materials supporting counterterrorism efforts, the Reasonable Belief Statement will specify whether the product or report contains Terrorist Threat Information or Vulnerabilities Information as explained in the Implementation Guidance, or otherwise informs an understanding of terrorism, along with an explanation as to how the information in the product or report falls within one or more of those categories.

(B) For covered materials referencing or concerning domestic violent extremists or homegrown violent extremists, the Reasonable Belief Statement will specify the basis for I&A's belief that each individual referenced is a domestic violent extremist, homegrown violent extremist, or international terrorist consistent with the criteria set forth in the Implementation Guidance.

(C) For covered materials concerning hate crimes, the Reasonable Belief Statement will specify how the information in the covered material at issue—

(I) Furthers an understanding of violent hate crimes as that term is explained in the Implementing Guidance;

(II) Otherwise furthers an understanding of terrorism, or consists of statistical or other aggregated information about hate crimes in general that furthers an understanding of violent hate crimes; or

(III) Supports a request for information concerning hate crimes from another departmental component, office, or element.

(D) For covered materials supporting efforts to protect critical infrastructure or key resources (CIKR), the Reasonable Belief Statement will specify how the information in the product or report is CIKR Information as explained in the Implementation Guidance, including how such information—

(I) Concerns a threat to destroy or incapacitate, or vulnerability to destruction or incapacitation, of a system, asset, or resource owned or operated by a Systemically Important Entity (SIE); or

(II) A threat to destabilize, or vulnerability to destabilization, of one or more national critical functions.

(E) For covered materials concerning mass casualty attacks, the Reasonable Belief Statement will specify how the attack(s) (or threat thereof) involves (or is reasonably likely to involve) multiple victims attacked indiscriminately (i.e., not motivated by any personal, financial, or other interest specific to the victims of the attack).

(F) For covered materials concerning mass violence as that term is explained in the Implementation Guidance, the Reasonable Belief Statement will specify—

(I) For reporting on mass violence, why I&A personnel believe the violence at issue is beyond the capabilities of affected state and local governments to effectively respond such that federal assistance is necessary; or

(II) For reporting on potential mass violence, any specific, objective facts or circumstances that when considered in isolation or tandem, indicate violent crime that would be beyond the capabilities of affected state and local governments to effectively respond such that federal assistance would be necessary.

(G) For covered materials concerning DHS protective activities as that term is explained in the Implementation Guidance, the Reasonable Belief Statement will specify the personnel, facilities, or operations subject to the reporting and how they fall within DHS's protective activities.

(d) Compliance Audits. The D/TOPO, acting through the Privacy and Intelligence Oversight Officer, will conduct regular audits of Reasonable Belief Statements to ensure their

consistency with the Intelligence Oversight Guidelines, their Implementation Guidance, and this policy guidance.

(e) Access to Reasonable Belief Statements. I&A personnel will provide copies of the Reasonable Belief Statements to the Office of the General Counsel's Intelligence Law Division, the DHS Privacy Office, the DHS Office for Civil Rights and Civil Liberties, and TOPO's Privacy and Intelligence Oversight Branch (collectively, the Oversight Offices) for any covered materials reviewed by those offices prior to dissemination outside DHS, or to any Oversight Office upon request.

1-203: Information Systems and Bulk Data Holdings Audits

On May 4, 2023, the Office of Intelligence and Analysis (I&A) established the Transparency and Oversight Program Office (TOPO) to consolidate and elevate all transparency and oversight functions within I&A. The Director of TOPO (D/TOPO) is responsible for working to ensure that all compliance audits required by law or policy, including I&A's Intelligence Oversight Guidelines, are conducted in a regular and timely manner. At the same time, legacy I&A systems are not necessarily designed to facilitate systems audits of the type envisioned in the Intelligence Oversight Guidelines, and any technical upgrades to those systems, or integration of auditing capabilities into future systems, must also be done consistent with available resources. Accordingly, this policy guidance establishes a foundation from which I&A can strengthen the oversight processes and technical capabilities that ensure its systems and data holdings are maintained and operate in a manner that conforms to the Constitution and laws of the United States and safeguards privacy, civil rights, and civil liberties:

(a) Responsible Official for Compliance Audits. I designate the D/TOPO as the I&A official responsible for compliance audits of I&A information systems and bulk data holdings containing U.S. Persons Information for consistency with the Guidelines. The D/TOPO will carry out this responsibility through the Privacy and Intelligence Oversight Officer and their staff in TOPO's Privacy and Intelligence Oversight Branch (TOPO/PIOB). The results of these compliance audits will be submitted to the Under Secretary for Intelligence and Analysis (USIA), the Associate General Counsel for Intelligence, the Chief Privacy Officer, and the Officer for Civil Rights and Civil Liberties.

(b) Support to Compliance Audits.

(i) All I&A personnel will support the D/TOPO in the execution of compliance audits of I&A information systems and bulk data holdings to the greatest extent possible, including by providing records, access to information, or personnel for interviews upon request.

(A) Each directorate, division, or center within I&A, on an ongoing basis, will identify and catalog information systems under their control that contain Personally Identifiable Information (PII).

(B) As part of this assessment and inventory, the directorates, divisions, and centers will determine whether these information systems contain identifying information about U.S. persons (U.S. Persons Information (USPI)) and, if so, whether any of the USPI is part of a bulk data collection, meaning a large collection of data that, due to technical or operational considerations, was acquired without the use of discriminants (e.g., specific identifiers or selection terms).

(C) The directorates, divisions, and centers will notify TOPO/PIOB and the Technology and Data Services Directorate within the Office of Management of any

- information systems containing USPI, including USPI in bulk data collections, on a rolling basis.
- (D) I&A personnel are encouraged to consult with TOPO/PIOB or the Office of the General Counsel's Intelligence Law Division (OGC/ILD) in making these assessments.
- (ii) The Deputy Under Secretary for Management (DUS/M), acting through D/TDS, will provide technical support to the D/TOPO in the conduct of compliance audits to the extent possible given available technical capabilities and resources, including by treating the capability to support such compliance audits as a requirement for the development or acquisition of new I&A systems and upgrades to existing systems.
- (c) Processes to Support Future Bulk Data Holdings Audits. To help ensure the Privacy and Intelligence Oversight Officer has sufficient awareness of I&A bulk data transfers and holdings to conduct bulk data holdings audits in the future—
- (i) All proposed bulk data transfers to or from I&A will be reviewed by the Data Access Review Council (DARC) prior to execution, among other reasons, to ensure the proposed data transfer constitutes a bulk data transfer within the meaning of the Guidelines;
- (ii) The DUS/M, acting through the D/TDS, will ensure that the Privacy and Intelligence Oversight Officer or their staff are invited to participate in any DARC reviews of I&A bulk data transfer requests, including by participating in DARC meetings;
- (iii) The DUS/M and the D/TOPO will jointly ensure that any terms and conditions governing bulk data transfers to or from I&A are approved by the USIA (and not someone delegated the authority to do so by the USIA) as required by the Guidelines; and
- (iv) The DUS/M, acting through the D/TDS, will develop a data management plan for each bulk data transfer reviewed by the DARC and approved by the USIA, which will include all relevant dates for actions required by the terms and conditions governing those transfers such as deadlines for auditing, data retention, and requests for extensions of existing deadlines.

1-204: Safeguarding Personal Information Collected From Signals Intelligence Activities

This policy guidance implements the requirements of Executive Order No. 14,086, *Enhancing Safeguards for United States Signals Intelligence Activities* (Oct. 7, 2022) and Presidential Policy Directive-28, *Signals Intelligence Activities* (Jan. 17, 2014), as amended by National Security Memorandum-14, *Partial Revocation of Presidential Policy Directive 28* (Oct. 7, 2022).

(a) Consistency With Law and Policy. Pursuant to Section 1.7(i) of Executive Order No. 12,333, *United States Intelligence Activities* (as amended June 30, 2008), Office of Intelligence and Analysis (I&A) personnel collect (overtly or through publicly available sources), analyze, produce, and disseminate information, intelligence, and counterintelligence to support national and departmental missions. I&A is not authorized to conduct—and does not conduct—signals intelligence collection activities.

(i) *Mission Support Requirement*. I&A personnel retain and disseminate personal information obtained through signals intelligence only to the extent that such information relates to an authorized national or departmental intelligence requirement.

(ii) *Privacy and Civil Liberties Safeguards*. The safeguards contained in the following guidance implement the principles contained in subsections (a)(ii) and (a)(iii) of Section 2 of Executive Order No. 14,086.

(b) Minimization. I&A does not have access to unevaluated or unminimized signals intelligence, including signals intelligence collected in bulk, but it may receive, from other Intelligence Community elements, signals intelligence information that has been evaluated or minimized, including information included in information reports or intelligence products subject to the provisions of Executive Order 14,086, among other requirements.

(i) *Dissemination*. I&A disseminates personal information of non-U.S. persons collected through signals intelligence activities only if dissemination of comparable information concerning U.S. persons would be permitted under Section 2.3 of Executive Order No. 12,333.

(A) I&A disseminates personal information concerning a non-U.S. person on the basis that it is foreign intelligence only if the information relates to an authorized intelligence requirement and not solely because of the person's foreign nationality or country of residence.

(B) Unless it possesses specific information to the contrary, I&A presumes that any evaluated or minimized signals intelligence information it receives from other Intelligence Community elements that have adopted procedures to implement Executive Order No. 14,086 meets this standard.

(C) I&A disseminates such information within the U.S. Government only if an authorized and appropriately trained individual has a reasonable belief that the

personal information will be appropriately protected and that the recipient has a need to know the information.

(D) I&A takes due account of the purpose of the dissemination, the nature and extent of the personal information being disseminated, and the potential for harmful impact on the person or persons concerned before disseminating personal information collected through signals intelligence to recipients outside the U.S. Government, including a foreign government or international organization. Personal information collected through signals intelligence activities is not disseminated for the purpose of circumventing the provisions of Executive Order No. 14,086.

(ii) *Retention.* As required by Executive Order No. 14,086, I&A retains personal information of non-U.S. persons collected through signals intelligence activities only if retention of comparable information concerning U.S. persons would be permitted under applicable U.S. law and deletes such information that may no longer be retained in the same manner that comparable information concerning U.S. persons would be deleted.

(A) I&A retains personal information concerning a non-U.S. person on the basis that it is foreign intelligence in accordance with applicable I&A and Intelligence Community policies and procedures, including the I&A Intelligence Oversight Guidelines, consistent with Section 2(c)(iii)(A)(2) of Executive Order No. 14,086, including that information relates to an authorized intelligence requirement and not solely because of the person's foreign nationality or country of residence.

(B) Unless it possesses specific information to the contrary, I&A presumes that any evaluated or minimized signals intelligence information it receives from other Intelligence Community elements that have adopted procedures to implement Executive Order 14,086 meets this standard.

(C) I&A retains such information in accordance with applicable record retention policies and subject it to the same retention periods that would apply to comparable information concerning U.S. persons.

(c) Data Security and Access.

(i) *General Requirements.* Access to all personal information collected through signals intelligence activities—irrespective of the nationality of the person whose information is collected—is restricted to those personnel who have a need to access that information in the performance of authorized duties in support of national or departmental missions and have received appropriate training on the requirements of applicable U.S. laws, as implemented by this policy and pursuant to Section 2(c)(iii)(B)(2) of Executive Order No. 14,086.

(A) Such information is maintained in either electronic or physical form in secure facilities protected by physical and technological safeguards, and with access limited by appropriate security measures.

- (B) Such information is safeguarded in accordance with applicable laws, rules, and policies, including those of I&A, DHS, and the Intelligence Community.
- (ii) *Classified Information.* Classified information is stored appropriately in a secured, certified, and accredited facility, in secured databases or containers, and in accordance with other applicable requirements. I&A's electronic system in which such information may be stored must comply with applicable law, executive order, and Intelligence Community and departmental policies and procedures regarding information security, including with regard to access controls and monitoring.
- (d) Data Quality. Personal information collected through signals intelligence activities—where such information can be so identified—is included in I&A intelligence products only as consistent with applicable Intelligence Community standards and analytic tradecraft, including such standards for accuracy and objectivity, as set forth in relevant directives, including Intelligence Community Directive 203, *Analytic Standards* (as amended June 12, 2023). Particular care should be taken to apply standards relating to the relevance, quality, and reliability of the information, consideration of alternative sources of information and interpretations of data, and objectivity in performing analysis.
- (e) Oversight.
- (i) *Periodic Review.* The Director of the Transparency and Oversight Program Office (D/TOPO), acting through the Privacy and Intelligence Oversight Officer, and in consultation with the Office of the General Counsel's Intelligence Law Division (OGC/ILD), reviews the implementation of this policy periodically, focusing particularly on relevant portions of Executive Order No. 14,086 regarding privacy and civil liberties, and reports to the Under Secretary for Intelligence and Analysis (USIA) regarding the application of the safeguards contained herein and in Executive Order No. 14,086 more generally, as applicable.
- (A) The Privacy and Intelligence Oversight Officers briefs their findings, provides copies of review reports to the Chief Privacy Officer and Officer for Civil Rights and Civil Liberties, and, as appropriate, consults with their offices on responsive steps to remediate any concerns identified through the reviews.
- (B) The D/TOPO serves as the primary point of contact with the Privacy and Civil Liberties Oversight Board regarding compliance with Executive Order No. 14,086, coordinating any such activity with the Chief Privacy Officer. TOPO, through its Privacy and Intelligence Oversight Branch (TOPO/PIOB), maintains an audit and compliance review procedure governing the periodic reviews described in Section 1-204(e)(i) above. I&A personnel are required to support any such reviews to the maximum extent possible.
- (ii) *Instances of Non-Compliance.* I&A personnel report instances of non-compliance with this policy guidance to TOPO/PIOB.

- (A) In consultation with OGC/ILD, TOPO/PIOB promptly reports instances of non-compliance to relevant entities to ensure their remediation and promptly reports significant instances of non-compliance with applicable U.S. law (i.e., systemic or intentional failures to comply with a principle, policy, or procedure of applicable United States law that could impugn the reputation or integrity of an element of the Intelligence Community activity, including in light of any significant impact on the privacy and civil liberties interests of the person or persons concerned) involving the personal information of any person collected through signals intelligence activities to the USIA, the Secretary, and the Director of National Intelligence, consistent with Section 2(d)(iii) of Executive Order No. 14,086.
- (B) TOPO/PIOB also provides notice of significant instances of non-compliance to the Department of Homeland Security (DHS) Privacy Office and DHS Office for Civil Rights and Civil Liberties.
- (f) Assistance to the Office of the Director of National Intelligence Civil Liberties Protection Officer. I&A personnel, acting through TOPO/PIOB, provide the Office of the Director of National Intelligence's Civil Liberties Protection Officer (ODNI/CLPO) with access to information necessary to conduct the reviews described in either Section 3(c)(i) or Section 3(d)(i) of Executive Order No. 14,086, consistent with the protection of intelligence sources and methods. I&A personnel do not take any action designed to impede or improperly influence the ODNI/CLPO's review of qualifying complaints or the Data Protection Review Court's review of the ODNI/CLPO's determination of such pursuant to the Signals Intelligence Redress Mechanism.
- (g) Assistance to the Privacy and Civil Liberties Oversight Board. I&A personnel, through TOPO/PIOB, provides the Privacy and Civil Liberties Oversight Board with access to information necessary to conduct the reviews described in Section 3(e)(i) of Executive Order No. 14,086, in consultation or coordination with the Chief Privacy Officer, as appropriate and consistent with the protection of intelligence sources and methods.
- (h) Training. All I&A personnel who have access to information that is subject to this policy will receive introductory and periodic training on applicable requirements, including reporting procedures. Successful completion of such training is a prerequisite to initial and continued access to information acquired through signals intelligence activities.
- (i) *Compliance With Training Requirement.* The Deputy Under Secretary for Management, through the Director of the Intelligence Training Academy (D/ITA) will monitor completion of this training requirement to ensure compliance with it.
- (ii) *Consultation and Support.* The D/TOPO, acting through the Privacy and Intelligence Oversight Officer, will consult with the D/ITA and provide subject matter expertise and support to the execution of the requirement set forth in Section 1-204(h)(i) above.

(i) Deviations From Policy Guidance. Deviations from this policy guidance are permitted only in accordance with the requirements set forth below.

(i) *Prior Approval.* The USIA must approve in advance any departures from this policy guidance after consultation with the Director of National Intelligence and the Assistant Attorney General for National Security following consultation with the Associate General Counsel for Intelligence (AGC/Intel).

(ii) *Exigent Circumstances.* If there is not time for prior approval and consultation and a departure from the procedures in this policy is necessary because of the immediacy or gravity of a threat to the safety of persons or property, or to national security, the USIA or their designee may approve a departure from these procedures.

(iii) *Notification.* The USIA, acting through the D/TOPO, reports any departures from the substantive provisions of this policy guidance pursuant to Section 1-204(f)(i)-(ii) above to the Chief Privacy Officer, the Officer for Civil Rights and Civil Liberties, and the AGC/Intel as soon after the departure as possible.

(A) The notification will include a brief explanation as to why exigent circumstances warranted the departure.

(B) Additionally, the AGC/Intel will provide prompt written notice of any such departures stating why advance approval was not possible and describing the actions taken to ensure activities were conducted lawfully to the Director of National Intelligence and the Assistant Attorney General for National Security.

(iv) *Lawfulness Required.* Notwithstanding the provisions for amendment or departure set forth above, all I&A intelligence activities must be carried out in a manner consistent with the Constitution and laws of the United States, including the requirements of Executive Order Nos. 12,333 and 14,086.

(j) Internal Guidance and Interpretation. These procedures are set forth solely for internal guidance within I&A. Questions on the applicability or interpretation of these procedures should be directed to OGC/ILD, who determines such applicability or interpretation, in consultation with the Department of Justice, as appropriate.

1-205: Disclosure of Section 1367 Information

This section is a placeholder. The policy will be included in a future version of the Policy Manual.

1-206: Special Handling Requirements for Congressional Identity Information

This section is a placeholder. The policy will be included in a future version of the Policy Manual.

1-207: Privacy and Civil Liberties Oversight Program

This section is a placeholder. The policy will be included in a future version of the Policy Manual.

1-208: Policy Coordination and Oversight

The Office of Intelligence and Analysis (I&A) requires a standardized, commonly understood policy process to continue to mature as an organization. I&A personnel cannot be expected to perform their work effectively without a clear understanding of the purposes, objectives, and prescribed activities of their respective programs, which requires an understanding of the policies and processes that govern those programs. That understanding, in turn, demands clear, well-coordinated, and timely policy that is communicated effectively to the workforce. Further, it is vital for the maturation and organizational health of I&A to maintain internal controls that help to enforce compliance with such policy through the issuance of implementation guidance such as concepts of operation, standard operating procedures, policy implementation handbooks, and reference guides.

To reach these goals, I&A is revising its policy process consistent with three key principles. First, policy development must be fair, transparent, thoughtful, and timely. Second, policy guidance must reflect the priorities and vision of senior leadership, be informed by the subject-matter expertise of I&A personnel relying on the guidance and incorporate feedback from oversight and relevant support offices to ensure it is sustainable and appropriate. Finally, I&A staff supporting policy development should not be the primary generators of policy content, but rather should oversee the coordination and memorialization of policy content, focusing on ensuring fidelity to the first two principles while helping to ensure policies are clear, complete, and can be followed.

The revised framework below reflects these principles by refining I&A's approach to policy development, approval, implementation, and maintenance. It simplifies the development and approval of policy content by replacing policy instructions and other highly stylized policy instruments with a single format—policy guidance memoranda. The framework relies on a mix of written and in-person coordination to provide earlier insight into policy development by senior leadership while both streamlining and maintaining meaningful opportunities for review by affected personnel and oversight offices. It also relieves policy content creators of the obligation to ensure appropriate formatting, coordination, and record-keeping of I&A policy, assigning those responsibilities to the Policy Coordination and Oversight Branch within the Transparency and Oversight Program Office (TOPO/PCOB). Going forward, TOPO/PCOB will serialize and maintain approved policy guidance memoranda and codify the content of those memoranda in a standing policy manual that is available to individuals within and outside I&A. The result is a bifurcation of the former process under which the offices of primary responsibility (OPRs) for policy content focus their efforts on content generation, while policy professionals focus on the content's refinement, memorialization, coordination, staffing, records management, and codification.

Accordingly, I&A policy, including policy guidance and implementation guidance, will be developed, coordinated, staffed for approval, serialized, maintained, and codified consistent with the provisions set forth below.

1-208-01. Foundational Concepts.

(a) Scope.

(i) This policy guidance governs the development, coordination, staffing, issuance, maintenance, implementation, and codification of I&A policy, defined by the Department of Homeland Security (DHS) as a “body of rules intended to influence decisions and actions,”³ and generally understood to mean “a definite course or method of action selected from among alternatives and in light of given conditions to guide and determine present and future decisions.”⁴

(A) I&A policy does not include external rules imposed on DHS such as requirements set forth in law, executive order, or presidential memorandum. Nor does it include choices made by DHS or other agencies with government-wide authority that I&A is bound to follow such as requirements set forth in regulation or in DHS policy. Those rules and choices may inform or even dictate I&A policy, but I&A policy, including the guidance on developing I&A policy set forth in this memorandum, is limited to choices made, and rules formulated, by I&A.

(B) Consequently, this memorandum does not apply to intelligence policy for the Department issued by the USIA in their capacity as the DHS Chief Intelligence Officer.

(ii) In addition to guidance concerning I&A policy, this memorandum also sets forth guidance concerning the development and maintenance of charters for I&A governance bodies, employee associations and affinity groups, and long-term working groups.

(b) Policy Guidance and Implementation Guidance. For purposes of policy development and formatting, I&A distinguishes between policy guidance and implementation guidance.

(i) Policy guidance refers to high-level plans furthering general organizational goals and the procedures necessary to enable or further them. It includes content previously reserved for directives or instructions as well as delegations of authority or the formal designations of officials to perform specific, identified roles. Generally, policy should be developed and memorialized as policy guidance when it—

³ U.S. Dept of Homeland Sec., Management Directorate, *DHS Lexicon Terms and Definitions* at 491 (2017 ed.), available at https://www.dhs.gov/sites/default/files/publications/18_0116_MGMT_DHS-Lexicon.pdf.

⁴ Merriam Webster Dictionary, available at <https://www.merriam-webster.com/dictionary/policy> (last visited Nov. 20, 2024).

- (A) Governs the activities of multiple subcomponents (the I&A Front Office (including the Intelligence Enterprise Program Office and TOPO) and Offices of Analysis, Partnerships, Collection, and Management) within I&A;
 - (B) Sets forth new responsibilities or large-scale initiatives for a subcomponent; or
 - (C) Otherwise is of a character that requires understanding by all or a significant portion of the I&A workforce to fulfill their work-related responsibilities.
- (ii) Implementation guidance refers to more detailed processes, procedures, and workflows that assist I&A personnel in applying and following policy guidance. It includes concepts of operation, standard operating procedures, policy implementation handbooks, and reference guides. Generally, policy should be developed and memorialized as implementation guidance when it—
- (A) Is specific to a subdivision or unit within a subcomponent;
 - (B) Implements—i.e., can be traced back to—existing policy guidance; and
 - (C) Is intended primarily to assist employees in the conduct of their day-to-day work rather than to establish a new direction, vision, or agenda for I&A.
- (iii) Within I&A, the Director of TOPO (D/TOPO), acting through TOPO/PCOB, is responsible for determining whether proposed policy should be developed and memorialized as policy or implementation guidance in consultation with the OPR for the subject matter of the proposed policy and subject to the guidance and direction of the USIA or PDUSIA.
- (iv) Policy guidance and implementation guidance are subject to separate process and formatting requirements as set forth in Section 1-208-02 through 1-208-03 below.

1-208-02. Policy Guidance.

- (a) Format for New Policy Guidance. I&A issues new policy guidance through serialized policy guidance memoranda (PGMs) using a standardized format, promulgated by TOPO/PCOB, containing content developed by the OPR for the topic of the policy guidance in consultation with TOPO/PCOB, and issued by the USIA.
- (i) Generally, PGMs are organized to provide the purpose of the policy guidance, background information necessary to understand the context of the guidance, the content of the guidance, and directions for implementation of the guidance. They do not contain separate sections for definitions or roles and responsibilities, which are listed instead in the Policy Manual.

(ii) The policy content and implementation sections are organized in outline form to facilitate ease of reference for specific policy provisions. The other sections of the PGMs are written in narrative form.

(iii) TOPO/PCOB maintains the authoritative I&A template for PGMs, a copy of which is attached to this memorandum. Sample PGMs are available to interested I&A personnel upon request.

(iv) To ensure a common understanding across I&A as to which PGMs are authoritative and eliminate rogue policies, all PGMs must be signed by the USIA (or PDUSIA on behalf of the USIA) and serialized by TOPO/PCOB to be deemed effective.

(b) Principles of Policy Guidance Writing. Other than the basic structure for PGMs delineated in Section 1-208-02(a) above, there are no categorical rules governing their content other than the need to adhere to any underlying parameters established by law, presidential guidance, regulation, or national, Intelligence Community, or departmental policy; however, to the greatest extent possible, PGMs should be drafted consistent with the following principles:

(i) The purpose of policy guidance is to inform I&A personnel on the priorities, practices, and procedures of the organization at a high level. Accordingly, the policy content for PGMs should focus on requirements, rules, and processes applicable across I&A rather than dwell on the roles and responsibilities of subdivisions or units.

(ii) Personnel within I&A and external stakeholders rely on policy guidance to obtain an accurate and up-to-date understanding of I&A's programs, projects, and activities. Accordingly, policy guidance should not be aspirational. OPRs seeking to impose new requirements on I&A personnel should explain, at least on a basic level, how those new requirements will be implemented and executed, or, absent that, when and how those details will be provided (e.g., through implementation guidance to be issued within a prescribed number of days).

(iii) To the greatest extent possible, terms of art and terms commonly used in policy guidance will be consistent across PGMs. For example, consistent with rules of construction used in legislation and presidential guidance, the term "coordinate" should always be used to connote approval whereas "consult" should always be used to connote notice and an opportunity to provide feedback. These terms of art will be explained in the Policy Manual or its lexicon.

(iv) PGMs should be written in plain language and consistent with commonly understood rules of grammar. Bullet points, sentence fragments, jargon, and excessive use of acronyms generally are disfavored.

(v) PGMs should follow DHS and I&A style guides, including restrictions and requirements concerning the appropriate use of DHS seals, emblems, and color palettes.

(c) Policy Guidance Development Process. PGMs are conceptualized, drafted, coordinated, staffed for signature, approved, serialized, communicated to the workforce, and codified in accordance with the “standard” or “ad hoc” workflow described in Section 1-208-02(c)(i)-(ii) below depending on the circumstances giving rise to the proposal for policy guidance.

(i) Standard Process. This is the default process for developing PGMs. It is used for all proposed policy guidance other than proposals that meet the criteria for the ad hoc process described in Section 1-208-02(c)(ii) below. There are seven stages of the standard process, which are coordinated, facilitated, and overseen by TOPO/PCOB. These stages are described below.

(A) *Stage One—Pre-Development:* Before initiating a proposal for policy guidance, the OPR seeking this guidance must obtain written authorization to pursue the guidance from their cognizant subcomponent head.

(B) *Stage Two—Policy Scoping:* The OPR presents its approved policy guidance proposal to TOPO/PCOB using a policy intake form provided by TOPO/PCOB. TOPO/PCOB then convenes a scoping meeting with the OPR to discuss the proposed policy guidance, develop a work plan for the PGM, and identify stakeholders for coordination. The nominal timeline for this stage is 2 working days.

(C) *Stage Three—Initial Drafting and Leadership Check-In:*

(I) After policy scoping is complete, the OPR writes a first draft of the policy content for the PGM using the template provided by TOPO/PCOB. Throughout the drafting process, TOPO/PCOB is available to assist the OPR in conceiving, organizing, formatting, and drafting the content upon request.

(II) Separately, TOPO/PCOB briefs the Corporate Management Board (or equivalent group) on the proposed policy guidance and solicits feedback on the proposal from I&A senior staff. This check-in provides I&A senior staff the opportunity to identify any previously unidentified equities in the proposed policy guidance and participate in its development.

The nominal timeline for this stage is 5 working days.

(D) *Stage Four—Coordination:* Once a draft PGM has been written, TOPO/PCOB shares the draft with the Office of the General Counsel’s Intelligence Law Division (OGC/ILD) and other stakeholders, including at the senior leadership level, for review and comment. Concurrently, TOPO/PCOB conducts its own review of the document for consistency with the formatting requirements set forth in Section 1-208-

02(a) above and the principles of policy drafting set forth in Section 1-208-02(b) above. The nominal timeline for this stage is 7 working days.

(E) *Stage Five—Adjudication and Final Leadership Check-In:*

(I) TOPO/PCOB works with the OPR, OGC/ILD, and stakeholders to adjudicate any feedback received through the coordination process, mutually resolving or elevating critical edits or concerns for resolution and revising the draft PGM consistent with favorably adjudicated edits and comments.

(II) Separately, TOPO/PCOB briefs the Corporate Management Board (or equivalent group) on the status and significant features of the revised draft PGM, soliciting feedback on the revised draft PGM from I&A senior staff. This check-in affords I&A senior staff the opportunity to raise any questions or concerns about the revised draft PGM prior to its finalization and staffing for signature.

The nominal timeline for this stage is 7 working days.

(F) *Stage Six—Form and Legality Review:* Following the final leadership check-in, TOPO/PCOB refers the revised draft PGM to the Associate General Counsel for Intelligence (AGC/Intel), requesting certification that the draft PGM is legally sufficient. Concurrently, the D/TOPO reviews the draft PGM and, where the requirements set forth in Section 1-208-02(a)-(b) above are satisfied, certifies that the draft PGM meets the formatting requirements for approval. The nominal timeline for this stage is 5 working days.

(G) *Stage Seven—Staffing for Signature and Serialization:*

(I) Where the revised draft PGM is certified by the AGC/Intel as legally sufficient and the D/TOPO as properly formatted, TOPO/PCOB transmits the draft PGM through I&A's Executive Secretariat (Exec Sec) to the Chief of Staff, PDUSIA, and USIA for review and, where approved, signature. Any concerns identified by any of these officials must be resolved before the draft PGM is resubmitted to Exec Sec to resume staffing the guidance for signature.

(II) Concurrently, TOPO/PCOB works with I&A communications staff and, as appropriate, the senior staff to develop a workforce communications plan for the PGM. This plan may range from actions as simple as the issuance of the enacted PGM to I&A personnel via e-mail to more sustained engagement through a town hall, "lunch and learn"-type events, briefings to specific subdivisions or units within I&A, supplemental written resources, or some or all of the above.

(III) Once the USIA signs the PGM, Exec Sec transmits the signed PGM to TOPO/PCOB for serialization and inclusion in the PGM repository maintained by TOPO/PCOB. At this point, the PGM is in effect and binding on I&A personnel.

(ii) Ad Hoc Process. This is an alternative process, coordinated, facilitated, and overseen directly by the D/TOPO with the OPR, OGC/ILD, and I&A stakeholders at the principals level, used for more sensitive, high-profile, or expedited policy guidance requests or proposals. The process used for such requests or proposals, to the greatest extent possible, will mirror the stages of the standard policy guidance development process, but the specific manner and sequencing of those stages will vary depending on the proposal. Generally, this process will be reserved for policy guidance requests or proposals that are—

(A) Required on an expedited timeline by Congress or the President or their staff;

(B) Directed or requested by the Secretary, Deputy Secretary, or USIA;

(C) Responsive to exigent taskings or expedited lines of effort agreed to through interagency process such as that conducted by the National Security Council staff; or

(D) Reasonably likely to have novel and unusually complex or significant implications for the privacy, civil rights, or civil liberties of the American people or special protected classes of individuals.

(d) Policy Guidance Codification. To emphasize maximum transparency within I&A and with external stakeholders—including Congress—and, as appropriate, the public, I&A, through TOPO/PCOB in partnership with I&A communications staff and TOPO's Freedom of Information Act (FOIA) Branch, maintains the Policy Manual, which codifies the content of I&A policy guidance.

(i) The Policy Manual will be a modular, digital document available to I&A personnel via I&A's intranet portal and the public via I&A's FOIA Reading Room and, to the extent practicable, the I&A page on DHS's public facing website.

(A) The Policy Manual will include an I&A lexicon of defined terms and a table of references for the manual as a whole and specific provisions within it.

(B) Except to the extent necessary to protect applicable privileges or safeguard sensitive sources or methods, the entirety of the Policy Manual will be made available to the public.

(ii) TOPO/PCOB will review the Policy Manual on at least a semiannual basis to ensure it is accurate and up to date, including by adding or incorporating the content of new policy guidance. The D/TOPO will review, coordinate with the relevant OPR(s) and

OGC/ILD, and certify to the USIA the accuracy and appropriateness of the codification of the content from new policy guidance in the Policy Manual. In addition, the D/TOPO will describe any proposed substantive edits to the Policy Manual identified through this review for the USIA's approval. The D/TOPO, acting through TOPO/PCOB, will communicate any updates to the Policy Manual to the I&A workforce.

1-208-03. Implementation Guidance.

(a) Types of Implementation Guidance. I&A personnel use different types of implementation guidance depending on the nature of the guidance pursued and the preferences of the I&A organizational unit pursuing them.

(i) Generally, there are four types of implementation guidance used by I&A personnel, as follows:

(A) *Concepts of Operation (CONOPs)* are used for proposed, new, or pilot initiatives. They help enable a common understanding of these initiatives by explaining the initiative's purpose, defining its parameters, explaining the processes and timelines for accomplishing it, and establishing specific, measurable, achievable, relevant, and time-bound objectives for success.

(B) *Standard Operating Procedures (SOPs)* list standing processes, procedures, and timelines used by I&A personnel to execute their assigned responsibilities in a consistent and effective manner.

(C) *Policy Implementation Handbooks* collect multiple SOPs for the same organizational unit within I&A in a single document for ease of use.

(D) *Reference Guides* articulate existing policy or implementation guidance in ways more conducive than PGMs to regular use by I&A personnel without expanding on the substance of that guidance.

(ii) Currently, there is no prescribed format for any of the types of implementation guidance described in Section 1-208-03(a)(i) above; however, to the extent helpful, I&A personnel are encouraged to use templates for each of those types of implementation guidance maintained by, and made available upon request to, TOPO/PCOB.

(b) Requirements for Implementation Guidance. Implementation guidance should be maximally useful to the I&A personnel who use it. It does not, however, require the same level of formatting consistency expected of higher level, more broadly applicable policy guidance. Consequently, there are fewer substantive and formatting requirements for implementation guidance. Nevertheless, the following basic requirements must be satisfied:

(i) Implementation guidance cannot contradict or undermine requirements or restrictions imposed by the Constitution, the laws of the United States, executive order or presidential memorandum, regulation, national or departmental policy, or the direction of any U.S. government official or agency with authority over the conduct of I&A personnel.

(ii) Implementation guidance must identify the underlying policy guidance—whether national, Intelligence Community, departmental, or I&A—that it seeks to implement. The scope of the implementation guidance may not exceed the scope of its underlying policy guidance.

(A) I&A personnel are encouraged to consult with OGC/ILD or TOPO/PCOB should they require assistance in identifying or understanding the scope of the implementation guidance’s underlying policy guidance.

(B) Draft implementation guidance that is authorized by law, but lacks underlying policy guidance to implement, may be formatted and processed as policy guidance instead, consistent with Section 1-208-02 above.

(iii) Consistent with Section 1-208-03(a)(i)(A) above, every CONOP should explain the initiative’s purpose, define its parameters, explain the processes and timelines for accomplishing it, and establish specific, measurable, achievable, relevant, and time-bound objectives for success.

(c) Implementation Guidance Development Process. Except where a higher level of approval is required by law or other applicable policy, implementation guidance, following review by OGC/ILD and TOPO/PCOB, may be issued by the head of any subcomponent, or, where authorized in writing by their cognizant subcomponent head, any head of a directorate, center, or division within that subcomponent (collectively, Approval Officials).

(i) Any organizational unit within I&A may serve as the OPR for the implementation guidance, drafting its text as it sees fit; however, the OPR may, in its discretion, seek assistance from TOPO/PCOB in drafting such guidance, and OPRs are encouraged to rely on templates maintained by TOPO/PCOB to help draft the guidance.

(ii) Before submitting draft implementation guidance for approval by its cognizant Approval Official, the OPR must refer the draft implementation guidance to TOPO/PCOB, which will both review the draft guidance and coordinate its review with OGC/ILD for compliance with Section 1-208-03(b) above within ten working days of receipt of the draft guidance. Consistent with its responsibilities under Section 1-208-01(b)(iii), TOPO/PCOB will also review the draft guidance to determine whether it is properly characterized as implementation guidance or should be formatted and processed as policy guidance instead.

- (A) Any non-critical edits suggested by TOPO/PCOB or OGC/ILD will be adjudicated by the OPR in its discretion.
- (B) Any critical edits required by TOPO/PCOB or OGC/ILD must either be resolved to the satisfaction of the objecting element or elevated for resolution, as appropriate.
- (iii) Following adjudication or resolution of any edits from TOPO/PCOB or OGC/ILD, the OPR may refer the draft implementation guidance to its cognizant Approval Official for review and, as appropriate, approval, with copies of the referral, including the draft guidance referred to the Approval Official, provided to TOPO/PCOB and OGC/ILD.
 - (A) If the Approval Official approves the implementation guidance as drafted, the Approval Official signs the guidance and transmits it to TOPO/PCOB for serialization and inclusion in an I&A repository of authoritative implementation guidance maintained by TOPO/PCOB.
 - (B) If the Approval Official makes edits to the draft implementation guidance, those edits must be reviewed by TOPO/PCOB and OGC/ILD prior to incorporation in the draft implementation guidance consistent with the process described in Section 1-208-03(c)(ii) above.
 - (C) If the Approval Official disapproves the implementation guidance, the matter is considered closed pending any further action by the Approval Official or the OPR.
- (iv) If and when implementation guidance is both signed by the cognizant Approval Official and serialized and maintained by TOPO/PCOB consistent with Section 1-208-03(c)(iii)(A) above, the guidance will be in effect and transmitted to the OPR for execution.

1-208-04. Charters. A charter is a formal policy document outlining the structure, roles, rules, and processes for groups established to carry out existing responsibilities or authorities.

- (a) Applicability. Charters are required for any I&A governance body; employee associations or affinity groups; or working groups operating on an enduring or long-term (i.e., for at least one year) basis (collectively, Charter Groups).
- (b) Required Contents for Charters. All charters subject to this guidance consistent with Section 1-208-04(a) above must contain the following:
 - (i) The Charter Group's official name;
 - (ii) The legal authority and any applicable policy guidance under which the Charter Group is established;

- (iii) The objective and scope of the Charter Group's activities;
- (iv) A description of the duties for which the Charter Group is responsible;
- (v) The organizational unit or official within I&A responsible for providing logistical and administrative support to the Charter Group;
- (vi) The structure and organization of the Charter Group, including its chair and any co- or vice-chairs, membership, and any non-participating observers, which must include participation (or the opportunity to participate) by OGC/ILD;
- (vii) The rules by which the Charter Group operates, including the selection of its chair, any co- or vice-chairs, members, and any observers; the frequency and functioning of its meetings; and the manner in which Charter Group decisions, recommendations, or findings are made, memorialized, maintained for records management purposes, and made available to others, including with respect to whether sub-groups may be created and, if so, by whom and how they will operate with respect to the Charter Group;
- (viii) The expected duration of the Charter Group; and
- (ix) The procedures by which the charter may be amended or terminated.

(c) Charter Development Process. Charters must be reviewed for approval by the USIA following review by OGC/ILD and TOPO/PCOB.

- (i) Any organizational unit within I&A may serve as the OPR for a charter, drafting its text as it sees fit; however, the OPR may, in its discretion, seek assistance from TOPO/PCOB in drafting the charter, and OPRs are encouraged to rely on templates maintained by TOPO/PCOB to help draft the charter.
- (ii) After completing an initial draft of a charter, the OPR must refer the draft charter to TOPO/PCOB, which will both review the draft charter for compliance with Section 1-208-04(b) above not later than ten working days following receipt of the draft charter and refer the draft charter to OGC/ILD for legal sufficiency review. TOPO/PCOB will also review the draft charter to determine whether it adheres to principles of fairness and transparency, including (and especially) with respect to how decisions, recommendations, and findings are made by the Charter Group to ensure no single office or official within I&A exercises disproportionate influence on the group's decisions.
 - (A) Any non-critical edits suggested by TOPO/PCOB or OGC/ILD will be adjudicated by the OPR in its discretion.
 - (B) Any critical edits required by TOPO/PCOB or OGC/ILD must either be resolved to the satisfaction of the objecting element or elevated for resolution, as appropriate.

(iii) Following adjudication or resolution of any edits from TOPO/PCOB or OGC/ILD, TOPO/PCOB will refer the draft charter to the USIA via Exec Sec for review.

(A) If the USIA approves the charter as drafted, the USIA will sign the charter and transmit it to TOPO/PCOB for serialization and inclusion in an I&A repository of charters maintained by TOPO/PCOB.

(B) If the USIA makes edits to the charter, TOPO/PCOB will coordinate the review of those edits by the OPR and OGC/ILD for any additional edits or comments before resubmitting the revised charter to the USIA.

(C) If the USIA disapproves the charter, the matter is considered closed pending any further action by the USIA or the OPR.

(iv) If and when the charter is both signed by the USIA and serialized and maintained by TOPO/PCOB consistent with Section 1-208-04(c)(iii)(A) above, the charter will be in effect and transmitted to the OPR for execution.

1-208-05. Rogue Instruments. Policy guidance, implementation guidance, and charters developed after this memorandum's effective date must be approved by the USIA or designated Approval Official and serialized by TOPO/PCOB consistent with Section 1-208-02 through 1-208-04 above for the instrument to bind I&A personnel. Rogue instruments not approved or serialized in accordance with this policy guidance will be considered for approval, as appropriate, consistent with the requirements and processes described in Section 1-208-02 through 1-208-04 above, but will not be considered authoritative or operational unless and until approved and serialized consistent with this memorandum. I&A personnel should refer any rogue instruments they encounter to TOPO/PCOB for processing consistent with this guidance.

1-209: Internal Controls

This policy guidance establishes the roles, responsibilities, and procedures for the Internal Controls Program within the Office of Intelligence and Analysis (I&A). Internal controls are systematic processes used by management to help an organization achieve its objectives. The Internal Controls Program allows leadership to provide reasonable assurance that the organization is operating effectively and efficiently, complying with policy and law, and reporting reliably.

Federal agencies are required to implement mechanisms to assess internal controls and enterprise risk, and all Department of Homeland Security (DHS) components are required to develop procedures and internal controls to improve effectiveness, efficiency, and accountability and comply with DHS organizational performance management guidance. All I&A personnel have a role to play in ensuring that I&A establishes and complies with internal control requirements. Senior leadership has a special responsibility to ensure that all stakeholders meet their accountability requirements.

Within I&A, the Internal Controls Program is overseen by the Director of the Transparency and Oversight Program Office.

(a) Applicability. Internal controls are applied to each of I&A's key functions. This includes mission-critical operations such as analysis and collection as well as financial reporting and other core business functions like technology and data services. Internal controls apply to every subdivision and unit within I&A, allowing the organization to better understand and mitigate enterprise risk.

(b) Documenting Key Processes and Products. Key Processes and Products (KPPs) are the processes and products that have a material effect on a significant operation or are required to be conducted in compliance with law, regulation, policy, or some other binding obligation. The Internal Controls Program will provide training and assistance to aid in evaluating potential KPPs. In coordination with affected I&A subdivisions and units, the Internal Controls Program will—

- (i) Identify and catalog KPPs throughout I&A; and
- (ii) Identify internal control points of contact, who will be the primary interfaces for that I&A subdivision or unit with the Internal Controls Program.

The Internal Controls Program will consider entity level controls when identifying the KPPs. The Internal Controls Program is responsible for facilitating the integration of entity level control activities into KPPs, including by using the data collected during Intelligence Community assessments to identify, prioritize, validate, and mitigate intersecting risk.

(c) Routine Monitoring. The Internal Controls Program assesses internal control performance through routine monitoring, which focuses on the concept of continuous improvement rather than taking a reactionary approach as audit findings are issued.

- (i) After identifying and prioritizing I&A's KPPs, the Internal Controls Program will design a routine monitoring strategy that allows for updated baseline documentation; identifies and prioritizes risk(s) for monitoring; targets and remediates unmitigated risk(s) throughout the year; tests and validates remediation and corrective action; and supports assertion of internal control effectiveness.
 - (ii) The Internal Controls Program provides quarterly updates to the Corporate Management Board on the status of internal controls and shares its findings from routine monitoring. Through the Corporate Management Board, I&A determines corrective actions and ensures appropriate risk mitigation for I&A's KPPs.
- (d) Annual Assessment. DHS and the Office of Management and Budget require that I&A conduct annual compliance assessments of its internal controls for all significant financial and non-financial operations.
- (i) I&A monitors and remedies any deficiencies to obtain "reasonable assurance" that internal controls are established and effectively preventing significant weaknesses that would adversely affect organizational outcomes.
 - (ii) The Internal Controls Program incorporates Entity Level Control criteria into the assessment process to identify, prioritize, validate, and mitigate intersecting risk across I&A.
 - (iii) The Internal Controls Program develops an annual assessment scope and schedule for each fiscal year pursuant to the timelines prescribed by the DHS Risk Management and Assurance Internal Controls Over Financial Reporting (ICOFR) Process Guide. I&A offices may propose additional assessments for new or modified processes.
 - (iv) Using assessment results, the Internal Controls Program documents any material weaknesses and deficiencies. If the Internal Controls Program identifies an area in which a material weakness, significant deficiency, or internal control deficiency condition exists, the relevant I&A subdivision or unit develops, in coordination with the Internal Controls Program, a Mission Action Plan that provides correction and resolution of the issue.
 - (v) Pursuant to the timelines prescribed by the ICOFR Process Guide, the Internal Controls Program develops a Statement of Assurance to be issued by the USIA. The Statement of Assurance summarizes the overall adequacy and effectiveness of internal control within I&A, any known material weaknesses and areas of non-compliance, and corrective actions.

1-210: Interactions With the U.S. Government Accountability Office

This policy guidance governs the interactions of the Office of Intelligence and Analysis (I&A) with the U.S. Government Accountability Office (GAO), establishing the processes and procedures for responding to reviews by GAO concerning congressionally requested and government-wide GAO reviews of I&A. It assists I&A in following consistent business practices during the review process while complying with Intelligence Community and departmental policies, practices, and procedures.

At all times, it is the policy of I&A to cooperate with GAO to the fullest extent possible and provide timely responses to requests for information and documentation.

(a) Deconfliction of Policy Obligations. As both a Department of Homeland Security (DHS) component and an element of the Intelligence Community, I&A is subject to policy guidance issued both by the Department and the Office of the Director of National Intelligence (ODNI)—in particular, DHS Directive No. 077-02, *Relations With the U.S. Government Accountability Office* (as amended July 31, 2017), and DHS Instruction No. 077-02-001, *Relations With the U.S. Government Accountability Office* (as amended July 2, 2010), for DHS, and Intelligence Community Directive (ICD) 114, *Comptroller General Access to Intelligence Community Information* (June 30, 2011), for ODNI.

(i) Departmental policies concerning interaction with GAO generally have primacy with respect to I&A's engagements with GAO.

(ii) The exception to this general rule is with respect to requests for national intelligence information related to activities and programs funded wholly or in part by the National Intelligence Program (NIP), which is overseen by the Director of National Intelligence.

(b) Audit Officials. The Chief of Staff serves as I&A's Senior Component Accountable Official (SCAO), with responsibility for, and authority over, I&A audit and review activities. The SCAO, acting through the Director of the Transparency and Oversight Program Office (D/TOPO), oversees I&A's Component Audit Liaisons (CALs), who coordinate with the DHS Departmental Audit Liaison (DAL) to provide timely responses to GAO's requests.

(i) The CALs, in consultation with the D/TOPO or SCAO acting on behalf of the Under Secretary for Intelligence and Analysis (USIA), as appropriate, designate Designated Program Officials within the relevant subdivisions or units of I&A to serve as primary sources of information for GAO review teams during the review. Designated Program Officials may be contacted directly for records, information, and the scheduling of interviews during a GAO review.

(ii) The SCAO, D/TOPO, and CALs, in consultation with the Office of the General Counsel's Intelligence Law Division, work with GAO to ensure it receives access to requested information consistent with ICD 114 and applicable legal privileges.

(c) General Guidance for GAO Review.

(i) I&A facilitates GAO's review of national intelligence information related to NIP-funded activities or programs in accordance with ICD 114. Consistent with the ICD, I&A does not provide information on sensitive intelligence sources or methods.

(ii) Analytic products or other disseminated, strategic-level intelligence relevant to a GAO review, information relating to the administration of a government-wide program or activity, and publicly available information generally are provided to GAO.

(iii) Information that falls within the purview of the congressional intelligence oversight committees generally is not made available to GAO to support a GAO review of national intelligence capabilities and activities. This includes reviews of intelligence collection operations, intelligence analyses and analytic techniques, counterintelligence operations, and intelligence funding.

(iv) I&A does not categorically deny GAO access to information, nor does I&A withhold information solely because the information relates to a program that is funded wholly or in part by the NIP.

(A) If it is determined that GAO cannot have access to requested information in its current state consistent with ICD 114 or applicable legal privileges, I&A will work with GAO to explore alternative means to accommodate the request (e.g., producing a tearline, requesting declassification, or partial redacting or summarizing information).

(B) I&A will inform GAO via email, during interviews, and through the completion of technical and sensitivity comment forms, of confidentiality obligations regarding classified and For Official Use Only information.

(C) If I&A determines that a GAO request for information cannot be accommodated, I&A will advise GAO promptly of its inability to accommodate the request along with a written explanation for the basis of that conclusion. The D/TOPO will provide courtesy copies of these communications to the DAL and ODNI's Office of Legislative Affairs.

1-211: Protection of Sources and Methods Under the Freedom of Information Act

The Freedom of Information Act (FOIA)⁵ requires public disclosure of government records and information except when such disclosure is not in the public interest. The Act permits the withholding of government information in response to FOIA requests where that information falls within one or more exemptions delineated in the Act. One such exemption, known as the “(b)(3) exemption” because of the statutory provision in which it is located, permits the government to withhold information from disclosure where another statute requires that the matter be withheld from the public in such a manner as to leave no discretion on the issue or establishes particular criteria for withholding or refers to particular types of matters to be withheld.⁶

The Office of Intelligence and Analysis (I&A) is subject to two statutes that requires matters to be withheld from the public without discretion: 6 U.S.C. § 121(d)(9), which provides that any intelligence information under the chapter of the Homeland Security Act of 2002 establishing I&A and its responsibilities must be shared, retained, and disseminated consistent with the authority of the Director of National Intelligence (DNI) to protect intelligence sources and methods under the National Security Act of 1947; and 50 U.S.C. § 3024(i)(1), which requires the DNI to protect, and establish and enforce policies to protect, intelligence sources and methods from unauthorized disclosure.

I&A takes seriously its obligation to protect sensitive sources and methods consistent with the Homeland Security Act of 2002 and National Security Act of 1947. I&A also takes seriously its obligations to provide transparency about its activities and programs consistent with the FOIA. I&A therefore scrupulously applies the (b)(3) FOIA exemption in a tailored manner that reflects its lack of discretion with respect to the need to protect sources and methods. Specifically, I&A applies the (b)(3) exemption as follows:

(a) Review of Information for Potential Release.

- (i) I&A withholds material relating to sources or methods where the disclosure of the material would negate or materially impair the effectiveness of those sources or methods or otherwise would create material impediments to I&A’s information collection efforts, either now or in the future.
- (ii) If no such potential negation or material impairment can be articulated and no other statutory basis exists to justify redaction, the requested information will be released.
- (iii) When assessing sources or methods for possible disclosure under FOIA, I&A should consider, for example, whether the disclosure might—

⁵ 5 U.S.C. § 552.

⁶ *Id.* § 552(b)(3)(A)-(B). Statutes enacted after the date of enactment of the OPEN FOIA Act of 2009 must specifically cite to this paragraph of the FOIA for the exemption to apply.

- (A) Decrease the willingness of a human source or organization to provide information;
- (B) Undermine the viability of a database or other information repository; or
- (C) Allow an adversary to apply countermeasures that would prevent a collector from acquiring information.

(b) Communications Regarding Application of the Exemption. To ensure clarity and consistency in I&A's application the (b)(3) exemption, the Director of the Transparency and Oversight Program Officer, acting through the Chief of the FOIA Branch, and in coordination with the Office of the General Counsel's Intelligence Law Division, will provide sample language for use in correspondence with FOIA requesters and declarations explaining the withholding of sensitive sources and methods information.

1-212: Organizational Ombuds

The I&A Organizational Ombuds is an independent, neutral conflict resolution practitioner who provides an informal and confidential forum to help address real or perceived concerns raised by the I&A workforce. They are available to the I&A workforce for raising real or perceived concerns (both individualized and systemic) about the I&A organization, its personnel, agency policies and practices, morale, and mission environment. The Organizational Ombuds also may help to identify patterns and systemic issues confronting I&A employees. The Organizational Ombuds is distinct from I&A's Analytic Ombuds, who performs separate functions with respect to the conduct of I&A's analytic activities.

While the Organization Ombuds formally reports to the Director of the Transparency and Oversight Program Office (TOPO) for administrative purposes, functionally, the Organizational Ombuds reports directly to the Under Secretary for Intelligence and Analysis (USIA) and the Principal Deputy Under Secretary for Intelligence and Analysis (PDUSIA). They operate independently from the organizational structure of I&A, free from control, influence, or interference by any I&A employee in conducting ombuds duties. The Organizational Ombuds engages Intelligence Community and federal officials, including ombuds partners, to address issues of common concern that transcend organizational boundaries.

The Organizational Ombuds derives their authority in part from Title 5, United States Code, Part I, Chapter 5, Subchapter IV, "Alternative Means of Dispute Resolution in the Administrative Process." They adhere to the Code of Ethics and Standards of Practice of the International Ombudsman Association (March 17, 2022), and the International Ombudsman Association Best Practices: A Supplement to International Ombudsman Association Standards of Practice (October 2009). The Organization Ombuds represents I&A on the Interagency Alternative Dispute Resolution Working Group and Coalition of Federal Ombuds.

This policy guidance is intended to assist I&A personnel who seek to raise issues and concerns involving the I&A workplace through consultation with the Organizational Ombuds.

Consultation with the Organizational Ombuds under this policy must not be construed as a substitute for the formal grievance process, for resolving personnel matters that would be appropriately addressed with DHS's Employee Relations Office within the DHS Management Directorate's Office of the Chief Human Capital Officer, or for the reporting on potentially criminal matters to the Office of the General Counsel's Intelligence Law Division or TOPO's Privacy and Intelligence Oversight Branch for further referral, as appropriate.

- (a) Role of the Organizational Ombuds. The Organizational Ombuds conducts informal inquiries and conflict resolution measures in an impartial manner, free from initial bias and conflicts of interest. Impartiality does not preclude the Organizational Ombuds from making recommendations or developing an interest in securing systemic changes deemed necessary because of the process, or from otherwise being an advocate on behalf of a designated constituency. The Organizational Ombuds may become an advocate within I&A for change where the Organizational Ombuds process demonstrates a need for it.

(b) Organizational Ombuds Activities. The Organizational Ombuds engages with subdivisions and units across I&A to receive allegations about improprieties, identify complaint patterns and trends, explore non-adversarial approaches for resolving concerns, promote better communication, foster constructive dialogue, increase collaboration, improve transparency, and facilitate equitable outcomes.

(c) Organizational Ombuds Approach. The Organizational Ombuds collaborates with individuals or groups to develop options for, and facilitate resolution of, individual complaints or systemic concerns at the most appropriate level, including by making recommendations for resolution of such complaints and concerns to those who have the authority to act on them or by making referrals to other DHS resources or dispute resolution processes as appropriate. Use of the Organizational Ombuds is voluntary; it is not a required step in any grievance, complaint, or investigatory process.

(d) Confidentiality of Information. The communications and identities of I&A employees visiting the Organizational Ombuds to seek assistance (visitor information), along with any ombuds records associated therewith, are considered confidential to the greatest extent permitted by law and policy, and will only be disclosed by the Organizational Ombuds where there is a belief that there is imminent risk of serious harm to the visitor or other individuals, reason to believe an actual or imminent potential violation of federal criminal law has occurred or will occur, when necessary to defend against a formal complaint of professional misconduct, or otherwise where required by law.

(i) With a visitor's permission, the Organizational Ombuds may, in their discretion, share visitor information with others to facilitate resolution of the visitor's dispute.

(ii) To facilitate positive organizational change, the Organizational Ombuds may share with I&A leadership non-attributable information, including visitor information, shared in a manner that protects the identity of the visitor, about emerging trends, policy gaps, and patterns of problematic behavior involving I&A as an organization.

(iii) The I&A Ombuds reports to the USIA, either directly or through the PDUSIA, and operates independently from the organizational structure of I&A, free from control, influence, or interference or any I&A employee in conducting ombuds duties, and may consider or address relevant issues at all levels within I&A.

(e) Coordination With Workforce Management and Engagement. The Organizational Ombuds coordinates with I&A's Workforce Management and Engagement Division within the Office of Management (M/WM&E) to provide information on both informal and formal means of administrative redress available to I&A employees, such as the DHS Administrative Grievance System, the DHS Equal Employment Opportunity Alternative Dispute Resolution Program, the Equal Employment Opportunity administrative compliant process, and the Merit Systems Protection Board, as applicable. They also may coordinate with M/WM&E on available resources for employees and general support for employee wellness and resiliency.

(f) Limitations on the Organizational Ombuds. The Organizational Ombuds does not—

- (i) Act or consult as counsel or a representative, advisor, or advocate for the interest of any individual employee in any formal process;
- (ii) Voluntarily serve as party to any formal grievance or complaint process regarding workplace disputes or other matters disclosed to the Organizational Ombuds pursuant to this policy;
- (iii) Voluntarily participate in or perform any formal investigative or adjudicative function;
- (iv) Voluntarily serve as a witness or testify in any formal process;
- (v) Accept notice on behalf of, or act as, an agent of service for I&A (for clarity, contact with the Organizational Ombuds does not toll any prescribed filing or notice deadlines under an authorized DHS or other official redress forum, program, or system);
- (vi) Make binding or other management decisions, mandate policies, or adjudicate issues for or on behalf of the USIA, PDUSIA or any other I&A leader, manager, or supervisor;
- (vii) Compel or direct anyone to take specific action to resolve a workplace issue; or
- (viii) Exercise administrative, supervisory, or other control over any I&A employee, detailee, or assignee not otherwise appointed under the direct administrative supervision of the I&A Ombuds.

(g) Organizational Ombuds Resources. I&A employees, detailees, or assignees may access ombuds services, or request information about the Organizational Ombuds Program any of the methods described in the I&A Organizational Ombuds SharePoint site.

1-213: Whistleblower Protections

This section is a placeholder. The policy will be included in a future version of the Policy Manual.

UNCLASSIFIED

PART TWO: ANALYSIS

UNCLASSIFIED

2-101: Organization of the Office of Analysis

The Office of Analysis consists of approximately 200 analysts who generate I&A's finished intelligence products.

(a) Analytic Centers. The Office of Analysis is organized around four mission centers: the Counterterrorism Center, Nation-State Threat Center, Cyber Intelligence Center, and Transborder Security Center.

(i) *Counterterrorism Center*. The Counterterrorism Center is charged with providing timely strategic intelligence on terrorist threats, trends, and activities to I&A's federal, state, local, tribal, territorial, and private sector (FSLTTP) partners, the DHS Intelligence Enterprise, and to the Intelligence Community at the lowest possible classification level. The center comprises three branches: Homeland Threat Actors; Tactics, Emerging Capabilities & Critical Infrastructure; and Travel & Foreign Actors.

(ii) *Nation-State Threat Center*. The Nation-State Threat Center provides intelligence regarding the identification, assessment, and mitigation of threats from nation-state adversaries. Its analysis informs the foreign engagements, policy discussions, and economic security decisions of I&A's various partners. The center's analytic priorities manifest in its four branches: Trade & Supply Chain Resiliency, Technology Transfer, Foreign Investment, and Counterintelligence & Malign Influence.

(iii) *Cyber Intelligence Center*. The Cyber Intelligence Center provides analysis that supports cybersecurity and resilience for FSLTTP partners, including critical infrastructure stakeholders. It is comprised of three branches: Critical Infrastructure Cyber Threats, Nation State Cyber Threats, and Cyber Tactics & Technologies.

(iv) *Transborder Security Center*. The Transborder Security Center produces integrated intelligence aimed at combatting transnational organized crime networks and their facilitators. It focuses on combatting significant drug smuggling organizations, transnational gangs, human smuggling, weapon trafficking, illicit trade, and the movement of illicit proceeds on behalf of these criminal enterprises. TBS has two branches: Transnational Organized Crime, and Migration & Human Smuggling.

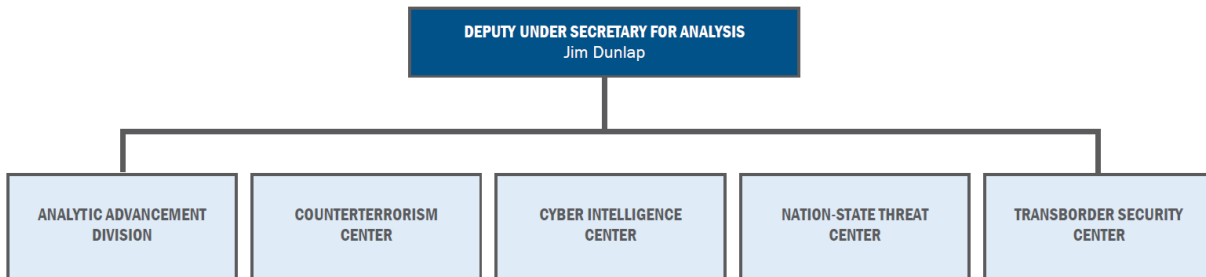
(b) Analytic Advancement Division. The Analytic Advancement Division (AAD) supports the analytic centers and their various missions. The AAD is responsible for ensuring I&A produces high-quality analysis relevant to homeland security stakeholders. It integrates executive-level review of finished products, guidance for producing finished intelligence, curation and briefing of intelligence to DHS principals and SLTT partners, departmental management of compartmented access programs, and dissemination and media services into one office. AAD has three branches: the Analytic Review Branch, Executive Support Operations, and the Design and Dissemination Branch.

(i) *Analytic Review Branch*. The Analytic Review Branch provides executive-level review and technical editing on finished intelligence products and analytic tradecraft training and support.

(ii) *Design and Dissemination Branch.* Design and Dissemination provides media service including graphic and cartography support as well as foreign disclosure and dissemination services.

(iii) *Executive Support Operations.* Executive Support Operations provides curation and briefing of current intelligence to DHS principals, the National Security Council, and FSLTTP partners as well as departmental management of compartmented access programs. Within Executive Support is the Homeland Enterprise Intelligence Support Team, which organizes daily briefings to connect intelligence personnel across the DHS Intelligence Enterprise and synchronizes analytic efforts around emerging threats.

The chart below depicts the organizational structure for the Office of Analysis.



2-102: Production of Finished Intelligence Products

The Office of Intelligence and Analysis (I&A) has an obligation to apply the best analytic standards and practices to all I&A finished intelligence products to ensure they effectively communicate analytic insight and are produced in a manner that is independent, objective, and maintains the highest analytic integrity. I&A also must adhere to law and applicable policy and appropriately protect individuals' privacy, civil rights, and civil liberties. To accomplish this, I&A conducts a review that focuses on both content and analytic tradecraft as well as compliance with oversight principles, guidelines, and procedures. This review process helps to ensure that I&A finished intelligence products (1) are issued in a timely manner; (2) conform to I&A's authorized missions, analytic tradecraft and qualitative standards, and legal, policy, and regulatory requirements; (3) protect the constitutional and privacy rights of U.S. Persons and other individuals; (4) respond to the requirements of I&A intelligence consumers; and (5) maintain the integrity of the intelligence process.

This policy guidance establishes the responsibilities and procedures within I&A for the production, review, approval, and dissemination of I&A finished intelligence products.

(a) Scope.

(i) This policy guidance applies to the production of finished intelligence products, meaning the physical manifestation, regardless of form or format, of analytic efforts conducted in furtherance of the I&A mission, which represent the analytic assessment, judgment, or other analytic input of I&A or intelligence personnel, are required to comply with Intelligence Community Directive 203, *Analytic Standards* (as amended June 12, 2023), and are intended to be disseminated outside of Department of Homeland Security (DHS) intelligence products that contain analytic conclusions.

(ii) It does not apply to the sharing of raw or unevaluated information or the analysis, production, or other assistance provided by intelligence personnel to support the authorized activities of DHS or non-DHS entities where no finished intelligence product is produced.

(iii) This policy guidance is not intended to replace or restrict other review, consultation, or oversight required by law or other authority, including that required by I&A implementing procedures for Executive Order No. 12,333, *United States Intelligence Activities* (as amended July 30, 2008).

(b) General Principles. I&A personnel must—

(i) Preserve at all times the independence and objectivity of intelligence, promptly reporting concerns of perceived politicization, interference with the intelligence production process, or other issues that compromise the integrity of intelligence analysis to the Deputy Under Secretary for Analysis, the I&A Analytic Ombuds, the Director of the Analytic Advancement Division within the Office of Management (D/AAD), or other cognizant authorities;

(ii) Successfully complete, and stay current on, applicable oversight, legal, and compliance awareness training; and

(iii) Seek advice from DHS subject-matter experts and offices when drafting I&A finished intelligence products, as appropriate.

(c) Content and Tradecraft Review. I&A finished intelligence products are reviewed by three levels, the first two within the analytic centers and the final review from AAD. The three levels of review collectively ensure every product addresses a relevant intelligence question, conforms to analytic tradecraft standards, and is well-written and well-reasoned.

(i) Product reviewers at the first level focus on the content of the product—its message and structure—and the analytic tradecraft informing the product’s analysis. First-level reviewers—typically team leads—ensure the product is clear; all evidence was considered; sources are described accurately; and variables, assumptions, and alternatives were explored. Products that fail to meet critical quality criteria are returned to the author for revision.

(ii) At the second level, the review perspective broadens. While second-level reviewers—typically senior intelligence officers—generally have less specific expertise, they have more awareness of the organization’s overall analytic production and its audience’s needs. They ensure the product’s message includes context and opportunities, builds on prior production, anticipates questions and addresses them, and is clear for the reader. Second-level reviewers are responsible for verifying that all criteria of first-level review were met; if not, the product is returned to the first level—and in some cases to the authors.

(iii) The third level is performed by the Executive Review Team within AAD. This level has the fewest sole responsibilities, but the most shared responsibilities, as it confirms that all criteria for a successful product have been met. By reviewing the piece from the perspective of an intelligence consumer, the executive reviewer can quickly gauge the readability of the piece—the goal is effortless comprehension—and how it compliments existing intelligence. Once this review is complete, the product should be clear, leave no obvious questions unconsidered, and reflect a consistent I&A corporate style and voice. If those or other criteria are unmet, the product is returned to previous levels of review.

(d) Oversight Equities Review.

(i) Some I&A finished intelligence products include information and analysis relating to U.S. persons, constitutionally protected activity, or other matters that have significant oversight equities. Products of this nature implicate the oversight equities of the Office of the General Counsel’s Intelligence Law Division (OGC/ILD), the DHS Privacy Office (PRIV), the DHS Office for Civil Rights and Civil Liberties (CRCL), and the Privacy and Intelligence Oversight Branch within I&A’s Transparency and Oversight Program Office (TOPO/PIOB) (collectively, the Oversight Offices). All I&A personnel, however, may

consult directly at any time with any or all of the Oversight Offices on any product to seek advice and comment or aid in determining whether a product meets one of these criteria or otherwise requires formal oversight equities review.

(ii) Prior to final approval and dissemination of a finished intelligence product outside DHS as described elsewhere in this policy guidance and further specified in the standard operating procedures for finished intelligence products, an oversight equities review by the Oversight Offices is required as prescribed in Section 2-102(d)(iv)-(v) below where the finished intelligence product—

(A) Addresses or describes populations discernable by race, ethnicity, gender identity, religion, sexual orientation, country of origin, or nationality;

(B) References or describes the activities of minors (under 18) individually or as a discernable population;

(C) Includes Personally Identifiable Information (PII) or identifies an individual by context;

(D) Reflects analysis based on or derived from a bulk data collection containing identifying information about U.S. persons (U.S. Persons Information (USPI)), meaning a large collection of data containing USPI that, due to technical or operational considerations, was acquired without the use of discriminants (e.g., specific identifiers or selection terms);

(E) Names elected government officials, candidates for elected office, or U.S. political parties;

(F) References or describes the political, religious, ideological, or constitutionally protected speech or activity of a U.S. person or person in the United States; or

(G) Falls within any additional bases for oversight equities review promulgated in writing by the DUS/A in coordination with the Oversight Offices.

(iii) All finished intelligence products that meet one or more of the criteria in Section 2-102(d)(ii) are provided to CRCL and the PRIV for review.

(A) I&A personnel work collaboratively with CRCL and PRIV to address any feedback. CRCL and PRIV comments require either resolution that is mutually acceptable to the submitting office or I&A elevation to the relevant mission manager where—

(I) CRCL identifies in writing that an I&A finished intelligence product does not adequately protect the civil rights or civil liberties of one or more individuals who are (1) U.S. persons or (2) located or suspected of being located within the United States and provides a written justification for the determination, which may include suggested revisions to reconcile the matter; or

(II) PRIV identifies in writing that an I&A finished intelligence product does not adequately protect the privacy of one or more individuals who are (1) U.S. persons or (2) located or suspected of being within the United States and provides a written justification for that determination, which may include suggested revisions to reconcile the matter.

(B) I&A analytic personnel address critical CRCL or PRIV comments in compliance with Intelligence Community analytic standards and may consult the Analytic Ombuds to discuss questions or concerns.

(iv) All finished intelligence products that meet one or more criteria in Section 2-102(d)(ii) also are provided to OGC/ILD and TOPO/PIOB for review.

(A) OGC/ILD comments require resolution that is acceptable to I&A personnel and legally sufficient or elevation to the relevant mission manager where OGC/ILD identifies in writing that a finished intelligence product does not comply with law, policy (including the Intelligence Oversight Guidelines or their Implementation Guidance), or otherwise determines the product to be legally objectionable and OGC/ILD provides a written justification for its determination, which may include suggested revisions to reconcile the matter.

(B) TOPO/PIOB comments require resolution that is acceptable to I&A personnel and complies with the Intelligence Oversight Guidelines and their Implementation Guidance or elevation to the relevant mission manager where PIOB identifies in writing that a finished intelligence product does not comply with the Intelligence Oversight Guidelines or their Implementation Guidance and TOPO/PIOB provides a written justification for its determination, which may include suggested revisions to reconcile the matter.

(C) I&A analytic personnel address critical OGC/ILD or TOPO/PIOB comments in compliance with Intelligence Community analytic standards and may consult the Analytic Ombuds to discuss questions or concerns.

(v) Those finished intelligence products that do not require oversight equities review pursuant to Section 2-102(d)(ii) may be advanced to the approval phase without oversight clearance unless an Oversight Office objects to, or raises a critical comment concerning, the finished intelligence product consistent with the criteria set forth in Section 2-102(d)(iii)-(iv) above and the Oversight Office provides a written justification for that determination, which may include suggested revisions to reconcile the matter.

(A) Objections or critical comments submitted pursuant to Section 2-102(d)(v) above may be resolved in a mutually acceptable manner at the staff level or elevated to the relevant mission manager.

(B) If resolution to the mutual satisfaction of I&A and the Oversight Office raising the objection or critical comment cannot be achieved by the mission manager, the

matter will be addressed through the dispute resolution process outlined in Section 2-102(g) below.

(vi) Notwithstanding Section 2-102(d)(i)-(iv) above, I&A personnel are authorized to advance finished intelligence products that meet one or more criteria in Section 2-102(d)(ii) to the approval phase if they have exhausted every reasonable effort to obtain required oversight office reviews and feedback or applicable clearance is not received within the timeframes prescribed in the I&A standard operating procedure for finished intelligence products, or as otherwise agreed to in advance between the Oversight Office(s) and either a cognizant product reviewer or the mission manager for that particular I&A finished intelligence product.

(e) Approval and Dissemination.

(i) The DUS/A or their designee conducts a final review and approves all I&A finished intelligence products for dissemination on behalf of the USIA, ensuring that all appropriate reviews, including oversight equities reviews, have been completed and the products satisfy all applicable standards and requirements, as appropriate.

(ii) All approved finished intelligence products are made available to the Oversight Offices prior to dissemination.

(f) Expedited Process. If a finished intelligence product relates to an exigent circumstance, the DUS/A may modify the processes described above in Section 2-102 as follows:

(i) If the expedited process is applied to an I&A finished intelligence product covered by Section 2-102(d)(ii) above, the DUS/A ensures the modified process allows the Oversight Offices the maximum amount of review and coordination time possible for the product to be released and still maintain its analytic value given the nature of the exigent circumstances giving rise to its production.

(ii) If the applicable review and approval processes cannot be completed within the timeframe deemed necessary by the DUS/A in Section 2-102(f)(i) above, every effort must be made to notify the relevant Oversight Office(s) prior to dissemination of that product, and I&A will send a copy of the disseminated product to the Oversight Offices.

(g) Dispute Resolution.

(i) In the case of a dispute between I&A and one or more Oversight Offices, the product reviewer and cognizant Oversight Office(s) should make a first attempt to resolve any critical edits, recalls, or revisions. If they cannot do so, the matter is elevated to the cognizant mission manager.

(ii) If the center director cannot resolve the issue, the matter is elevated to the DUS/A or their designee. The D/AAD and Analytic Ombuds assist in formulating a recommendation regarding the dispute to the DUS/A or their designee. If the DUS/A or their designee cannot resolve the dispute, the matter is elevated to the USIA for

resolution in consultation with the Associate General Counsel for Intelligence and the D/TOPO.

(A) If the matter is elevated to the USIA, the USIA reviews all the information to make a final determination for I&A. For finished intelligence products that meet one or more of the criteria of Section 2-102(d)(ii) above, the DUS/A recommends a resolution to the dispute to the USIA.

(B) In the event of a disagreement between the USIA and OGC/ILD, PRIV, or CRCL concerning the resolution of critical comments or revisions to a non-exigent I&A finished intelligence product, the USIA will hold dissemination of that product outside the Department temporarily while the USIA and head of the relevant Oversight Office(s) work expeditiously with the Deputy Secretary to resolve the critical concern.

(C) Following Deputy Secretary-level resolution, the USIA, as appropriate, incorporates revisions to content or other changes into a final version of the finished intelligence product for dissemination consistent with the Deputy Secretary's determination; informs the DUS/A and all Oversight Offices of those revisions; and provides them a final version of the product, which the DUS/A will then approve for dissemination.

(D) A record of the Deputy Secretary-level dispute resolution, along with copies of any findings, proposed revisions, and changes to the finished intelligence product—including a final version of the product approved for dissemination—will be submitted by the DUS/A, the D/AAD, and, through the cognizant mission manager, to the Analytic Ombuds to use and incorporate, as appropriate, into any reviews or reports described in Section 2-102(h) below.

(h) Post-Production Audits, Evaluations, and Quality Reviews.

(i) The D/AAD, in coordination with the Oversight Offices, maintains a process for conducting post-publication evaluations, audits, and reviews of I&A finished intelligence products to evaluate (1) analytic tradecraft and quality and (2) compliance with relevant oversight policies, guidelines, and principles directly related to their respective oversight authorities. The process for, and frequency of, these evaluations and audits should minimize the impact on production activities to the extent practicable while ensuring I&A provides appropriate support to the compliance review process consistent with the authorities of the Oversight Offices to inspect and review I&A materials as reflected in Executive Order No. 12,333 and Section 1-201-06 above.

(ii) The D/AAD, in consultation with the Oversight Offices, prepares periodic reports for I&A leadership based on substantive reviews of disseminated I&A finished intelligence products and any associated evaluations or audits during the respective reporting period. These reports will include—

- (A) An evaluation of finished intelligence products based on analytic tradecraft evaluations conducted by I&A;
- (B) An evaluation of compliance with relevant oversight policies, guidelines, and principles;
- (C) Any observations and examples of legal, oversight, or compliance concerns;
- (D) Incidents of substantive recalls or revisions summaries;
- (E) Details of elevated dispute resolution actions and outcomes;
- (F) Any recommendations for revised or new training or other measures of oversight and tradecraft principles to improve understanding and application; and
- (G) Any information deemed pertinent by the D/AAD, the Analytic Ombuds, or one or more of the Oversight Offices.

UNCLASSIFIED

PART THREE: COLLECTION

UNCLASSIFIED

3-101: Organization of the Office of Collection

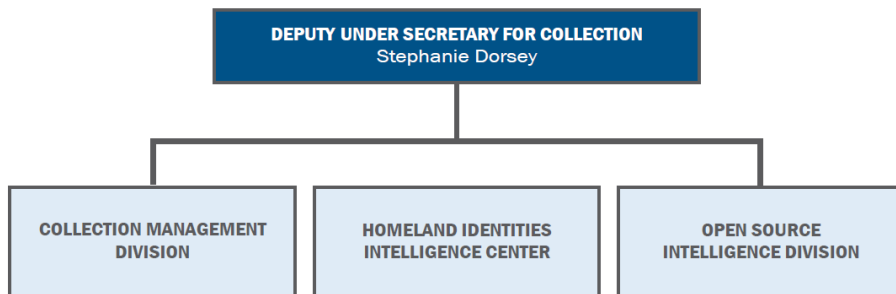
The Office of Collection within the Office of Intelligence and Analysis (I&A) oversees I&A’s collection and dissemination of intelligence to homeland security stakeholders. I&A’s collection activities focus on liaison collection from federal, state, local, tribal, territorial, and private sector (FSLTTP) partners, open-source collection, and identities intelligence to support the screening and vetting efforts of the Department of Homeland Security (DHS). The office is led by the Deputy Under Secretary for Collection.

The Office of Collection comprises three subordinate offices: the Collection Management Division, the Homeland Identities Intelligence Center, and the Open Source Intelligence Division.

(a) Collection Management Division (CMD). CMD leverages and manages the collection of all-source unevaluated (“raw”) intelligence to satisfy the requirements of DHS Intelligence Enterprise and Intelligence Community stakeholders. CMD represents DHS-wide equities across all intelligence collection disciplines through engagement with the Intelligence Community functional managers for each discipline.

(b) Homeland Identity Intelligence Center (HI2C). Identity intelligence is the ability to identify foreign or domestic actors who pose a threat to the homeland by fusing together unique DHS data with Intelligence Community information. HI2C manages discrete lines of effort to identify threat actors and enable Intelligence Community and federal law enforcement partners to take appropriate action.

(c) Open Source Intelligence Division (OSID). OSID collects information from publicly available online sources based on validated collection requirements for strategic collection. OSID also supports tactical collection for emerging threats to inform DHS leadership in coordination with the Intelligence Watch and Coordination Center. OSID identifies raw intelligence that informs finished intelligence production and its partners’ security posture. Because OSID’s reporting is derived from publicly available sources, analysts generally can share these insights at the unclassified level, increasing their utility for I&A’s FSLTTP stakeholders.



3-102: Open Source Intelligence Collection Program

Open source intelligence (OSINT), including publicly available information (PAI) on social media, is a critical means by which the Office of Intelligence and Analysis (I&A) supports the intelligence and information needs of the Department of Homeland Security (DHS) and its federal, state, local, tribal, territorial, and private sector (FSLTTP) partners. In just the past year, OSINT acquired by I&A has led to a greater understanding of, and informed federal, state, and local government actions in response to, terrorist threats, threats to critical infrastructure, and attempts to transfer sensitive technology outside the United States.

At the same time, much of the PAI of greatest intelligence value online consists of or includes speech or associational activities that lie at the heart of the First Amendment. I&A has a solemn obligation to uphold the rights of the American people when engaging in any intelligence activity, and these rights must be accounted for when collecting OSINT. To that end, I&A takes a measured approach to its collection of PAI, balancing DHS's compelling interest in obtaining and reporting such information with the need to safeguard privacy, civil rights, and civil liberties. I&A strikes that balance through the Open Source Intelligence Collection (OSIC) Program.

The OSIC Program consists of a small team of open-source collectors in the Open Source Intelligence Division (OSID) with subject-matter expertise in specific topics relevant to homeland security. Collectors in the program manually review publicly available social media and internet sites for information responsive to formal collection requirements, while remaining available to inform all-source reporting by the Intelligence Watch Coordination Center (IWCC) on emerging events. Where they identify such information, they memorialize the responsive information in unevaluated ("raw") single-source serialized reports known as Open Source Intelligence Reports (OSIRs) and periodically develop multiple-source serialized reports summarizing information with a common topic or theme called Open Source Intelligence Insights (OSIIs). These serialized reports are intended to provide raw intelligence that informs and helps I&A analysts identify strategic trends about homeland security threats and vulnerabilities that are published in analytic ("finished") products. The primary consumers of these finished intelligence products are FSLTTP partners with homeland security responsibilities as well as departmental leadership and other DHS components. Most OSIRs and OSIIs are made available to FSLTTP partners through the Homeland Security Information Network (HSIN).

The OSIC Program provides I&A personnel with the flexibility they need to gather information that helps protect against homeland security threats and vulnerabilities while safeguarding the privacy, civil rights, and civil liberties of the American people. I&A personnel participating in the OSIC Program are therefore expected to comply with the requirements and restrictions set forth in this memorandum at all times.

3-102-01. Scope and Focus.

(a) Activities Within the OSIC Program. The OSIC Program encompasses the collection of PAI from online sources, including social media, by dedicated OSINT collectors and their supervisors and managers in OSID (OSIC Personnel) in support of validated collection requirements to generate OSIRs or OSIIIs. It does not include the use of PAI by other I&A intelligence personnel. For example, it is distinct from the collection of PAI through liaison exchanges or field interviews, which is addressed through policies, processes, and standards applicable to the Field Intelligence Program (FIP), and from the collection of PAI in support of investigative or operational efforts to counter espionage and other foreign intelligence activities against the Department, which is conducted by I&A's Counterintelligence Program. The OSIC Program also does not include the overt acquisition of PAI (including online PAI) from third parties, nor does it include I&A's acquisition of, or access to, newspapers or other periodicals; books, journal articles, or other published works or reports; public filings or records; or similar documents or databases, whether accessed through a subscription or accessible free of cost.

(b) Authorized Personnel. Only OSIC Personnel may collect PAI online, including from social media, for serialization and release through OSIRs or OSIIIs (or equivalent reports).

3-102-02. General Requirements. All OSIC Personnel are subject to the general requirements set forth below.

(a) Compliance With Intelligence Oversight Guidelines. OSIC Personnel, like all I&A personnel, are required to follow I&A's Intelligence Oversight Guidelines when engaging in intelligence activities. This includes, but is not limited to, the following:

(i) OSIC Personnel are prohibited from engaging in any intelligence activity for the purpose of affecting the political process in the United States, for the sole purpose of monitoring activities protected by the First Amendment or the lawful exercise of other rights secured by the Constitution or laws of the United States, or for the purpose of retaliating against a whistleblower or suppressing or burdening criticism or dissent.

(ii) OSIC Personnel must reasonably believe that any intelligence activity furthers one or more of I&A's national or departmental missions to conduct them.

(iii) OSIC Personnel are prohibited from engaging in intelligence activities based solely on an individual's or group's race, ethnicity, gender, religion, sexual orientation, gender identity, country of birth, nationality, or disability. The use of these characteristics is permitted only in combination with other information, and only where (1) intended and reasonably believed to support one or more of I&A's national or departmental missions and (2) narrowly focused in support of that mission (or those missions).

(iv) OSIC Personnel may not request or direct any other person or entity to engage in any conduct prohibited by the Constitution, the laws of the United States, or Executive Order No. 12,333.

(b) Prohibition on Targeting Journalists. OSIC Personnel are prohibited from engaging in any collection targeting journalists in the performance of their journalistic functions.

(i) This prohibition applies to any individual gathering or editing news for presentation through any media regardless of whether the individual is employed by or acting on behalf of an accredited, certified, or otherwise professionally recognized media provider.

(ii) The prohibition applies to journalists when they are engaging in journalistic functions. Journalists engaging in non-journalistic activities, including any activity that violates federal criminal law, may be targeted for collection of intelligence or information concerning those non-journalistic activities to the extent the collection furthers a national or departmental mission and otherwise is permissible under I&A's Intelligence Oversight Guidelines and other applicable policies and procedures, including this policy guidance.

(iii) The prohibition applies to any collection of intelligence and information where a journalist's journalistic activities are the target or subject of the collection. It does not prohibit I&A from collecting intelligence or information from a journalist (or news organization), or PAI authored by and otherwise attributable to a named journalist, so long as the target of the collection is not a journalist engaging in journalistic functions.

(c) Prohibition on the Use of Personal Accounts. OSIC Personnel are prohibited from using personal accounts or registrations to access PAI online (including, but not limited to, PAI on social media) in furtherance of their official duties or responsibilities.

(d) Consistency With Collection Standards. OSIC Personnel must collect and report OSINT consistent with applicable Intelligence Community tradecraft standards and best practices, including, with respect to the sourcing and citation of PAI, the requirements set forth in Intelligence Community Directive 206, *Sourcing Requirements for Disseminated Analytic Products* (Jan. 22, 2015), and Intelligence Community Standard 206-01, *Citation and Reference for Publicly Available Information, Commercially Available Information, and Open Source Intelligence* (Dec. 2, 2024).

(e) Prohibition on Entering Into Terms of Service or User Agreements. OSIC Personnel are prohibited from entering into agreements or arrangements, including terms of service or user agreements, with publicly available online sources, including publicly available social media, in a manner that is incompatible with federal law, regulation, or policy, including the Anti-Deficiency Act, 31 U.S.C. § 1341 *et seq.*

(i) OSIC Personnel are prohibited from agreeing or consenting to terms of service or user agreements that contain unrestricted, open-ended indemnification provisions or clauses when registering for, or otherwise accepting access to, publicly available online sources, including publicly available social media.

(ii) OSIC Personnel should consult with the Office of the General Counsel's Intelligence Law Division (OGC/ILD) before agreeing or consenting to any terms of service or user agreement for a publicly available source, including publicly available social media, not previously agreed or consented to by I&A (including amended terms of service).

(f) Reproduction of Copyright Protected Materials. OSIC Personnel may only reproduce copyrighted works and materials in accordance with federal law, regulations, and policy, including the Copyright Act of 1976, 17 U.S.C. § 101 *et seq.* OSIC Personnel are encouraged to reach out to OGC/ILD with any questions regarding the application of copyright law to their intelligence activities.

(g) Fee-Based Services in OSINT. OSIC Personnel may procure fee-based services from publicly available online sources not otherwise available under the following circumstances:

(i) Any such procurement must be coordinated in advance with OGC/ILD, I&A's Financial Resources Management Division (FRM), and the Privacy and Intelligence Oversight Branch within the Transparency and Oversight Program Office (TOPO/PIOB).

(ii) Following coordination with OGC/ILD, FRM, and TOPO/PIOB, OSIC Personnel must submit their request to procure fee-based services from publicly available online sources to the Director of the Open Source Intelligence Division (D/OSID) for approval.

(iii) OSIC Personnel are prohibited from accessing "free trial offer" services from publicly available online sources unless approved by the D/OSID following coordination with OGC/ILD, FRM, and TOPO/PIOB consistent with the process described in Section 3-102-02(g)(i)-(ii) above.

(iv) Any such procurement must comply with Section 5-203 below.

3-102-03. Special Requirements for Social Media. In addition to the general requirements established in Section 3-102-02 above, OSIC Personnel are subject to additional requirements or restrictions when engaging in intelligence activities involving social media, meaning any publicly available online sites, applications, platforms, portals, wikis, blogs, virtual worlds, social bookmarking, web-based tools, or emerging technology used by people to express their beliefs, engage in dialogue, share information or media, collaborate, or otherwise interact. These requirements are in place to safeguard the constitutional rights of U.S. persons in their online activity.

(a) Limitation to Publicly Available Social Media. OSIC Personnel are limited to accessing and collecting intelligence and information from publicly available social media.

(i) Publicly available social media refers to social media that has been published or broadcast for public consumption, is available on request to the public, is accessible online or otherwise to the public, or is available to the public by subscription or purchase.

(ii) Social media that limits access using criteria that cannot generally be satisfied by members of the public is not publicly available social media.

(b) Prohibition on Focusing Collection on Constitutionally Protected Activities.

(i) As a best practice, OSIC Personnel do not focus their collection efforts on specific U.S. persons for collection except when providing tactical collection to amplify existing DHS efforts to gather all-source information about emerging events or exigent circumstances involving national or homeland security-related threats.

(A) Instead, OSIC Personnel access sites, platforms, or portals reasonably believed to contain PAI responsive to validated collection requirements supporting one or more authorized I&A missions.

(B) When accessing these sites, platforms, or portals, OSIC Personnel apply search terms reasonably calculated to retrieve PAI responsive to those validated collection requirements. These search terms are not focused on U.S. persons.

(i) Notwithstanding the limited scope and exigent nature of any efforts by OSIC Personnel to focus their collection on U.S. persons at all, to help ensure the protection of the constitutional rights of U.S. persons engaging in constitutionally protected activities online, OSIC Personnel are prohibited from focusing their collection on information concerning the political, religious, or ideological views or associations of U.S. persons from social media unless I&A personnel reasonably believe, based on information already available to them, that the U.S. person poses a terrorist or other threat to homeland security, or is associated with a person posing a terrorist or other threat to homeland security such that it is reasonable to believe that collection on the online activities of the potential subject of the collection will further an understanding of the threat posed by the potential subject's associate.

(ii) Prior to focusing any collection on a specific U.S. person from social media of information concerning their political, religious, or ideological views or associations, OSIC Personnel will prepare a written request to the D/OSID for authorization to engage in such collection. The request will explain why the OSIC Personnel believe the criteria set forth in Section 3-102-03(b)(i) above are satisfied.

(iii) OSIC Personnel will notify OGC/ILD and TOPO/PIOB of any requests under Section 3-102-03(b)(ii), including their accompanying explanations as to why they believe the criteria set forth in Section 3-102-03(b)(i) is satisfied, that are approved by the D/OSID as soon as is practicable, but in any event not later than three working days after approval of the request

(c) [Redacted.]

(d) [Redacted.]

(e) Exception. The rules, requirements, and restrictions set forth in Section 3-102-03(a)-(d) above do not apply to social media maintained by the federal government.

3-102-04. Certification. The starting point for participation in the OSIC Program is program certification. The certifications required for OSIC Personnel differ depending on the functions performed by those personnel.

(a) Certification for OSINT Collection. To be certified as eligible to conduct OSINT collection, OSIC Personnel must complete training developed or endorsed by I&A that enables them to collect and report PAI consistent with applicable Intelligence Community tradecraft standards and policies, including operational security tradecraft, the use of secure technologies to collect OSINT, and the production of OSIRs and OSIIs for appropriate audiences. OSIC Personnel must also complete their required intelligence oversight training consistent with Section 1-201-03(b) above.

(i) Previously, this training was delivered through OSINT training available to the I&A workforce and a separate workshop for potential OSINT collectors; per the direction of the USIA, the scope of OSID collector training is being evaluated. Following their review, the DUS/C, in consultation with the Deputy Under Secretary for Management (DUS/M) in their role overseeing training to I&A personnel, will determine whether the current training or a revised or replacement course satisfies the requirements set forth in Section 3-102-04(a) above.

(A) Until such time as the current training is revised or replaced, OSIC Personnel are deemed to have satisfied the training required by Section 3-102-04(a) above through successful completion of the training currently offered by I&A.

(B) As the current training is revised or replaced, OSIC Personnel must complete the revised or new training within one year of the availability of the revised or new training.

(C) The DUS/C may extend the training deadline set forth in Section 3-102-04(a)(i)(B) above.

(ii) Upon fulfilling their training requirements, OSIC Personnel submit a request for certification to engage in OSINT collection to their supervisors along with confirmation from the Intelligence Training Academy (ITA) that they have completed their required training, including intelligence oversight training. Their supervisors submit these materials through their chain of command to the D/OSID, who submits the request along with their recommendation on certification for decision by the DUS/C.

(iii) OSIC Personnel may not collect PAI online or draft any OSIRs or OSIIIs arising from such collection unless and until they are certified as eligible to collect OSINT by the DUS/C.

(b) Additional Certification for Certified Release Authorities. To be certified as eligible to approve the release of OSIRs in addition to collecting OSINT, OSIC Personnel, in addition to the requirements set forth in Section 3-102-04(a) above, must occupy a position within OSID designated to review and approve the release of OSIRs and complete specific training on the OSIR reporting process developed or endorsed by I&A.

(i) Previously, this training was delivered through the OSIR Certified Release Authority course; this training is being evaluated by the DUS/C, in consultation with the DUS/M (in their role overseeing and administering training to I&A personnel), for potential revision or replacement. Following their review of the OSIR Certified Release Authority course, the DUS/C will determine whether the OSIR Certified Release Authority course, either in its current or a revised form, or a replacement course, satisfies the requirements set forth in Section 3-102-04(b) above.

(A) Until the OSIR Certified Release Authority course is replaced or revised, OSIC Personnel are deemed to have satisfied the training required by Section 3-102-04(b) above by completing the OSIR Certified Release Authority course.

(B) If the OSIR Certified Release Authority course is revised or replaced, OSIC Personnel must complete the revised or new training within one year of the availability of the revised or new training.

(C) The DUS/C may extend the training deadline set forth in Section 3-102-04(b)(i)(B) above.

(ii) Upon fulfilling these requirements, OSIC Personnel submit a request for certification for release authority to their supervisors along with certification from the ITA that they have completed their required training. Their supervisors submit these materials through their chain of command to the D/OSID, who submits the request along with their recommendation on certification for decision by the DUS/C.

(iii) OSIC Personnel may not exercise release authority for OSIRs unless and until they are certified as release authorities by the DUS/C.

(c) Provisional Certification. In those rare circumstances where strict compliance with the requirements described in Section 3-102-04(a)-(b) above would materially impair I&A's capability to collect or report intelligence or information in furtherance of I&A's national or departmental missions, the DUS/C may provisionally certify I&A intelligence personnel who meet the requirements for certification other than those pertaining to training where the personnel, in the judgment of the DUS/C, have received equivalent training or developed sufficient experience such that they can collect and report OSINT or review draft OSIRs for release at the same level of proficiency as fully trained personnel. To the greatest extent practicable, provisionally certified personnel will be assigned to supervisory or managerial OSIC Personnel who have received the required training.

(i) Provisional certification must be memorialized by the DUS/C to go into effect and will remain effective for not more than one year from the date of provisional certification.

(ii) Personnel can only be provisionally certified once; thereafter, they must satisfy all requirements set forth in Section 3-102-04(a)-(b) above to retain their certification.

(iii) Under no circumstances may the DUS/C provisionally certify I&A intelligence personnel where those personnel have not completed the intelligence oversight training required under Section 3-102-04(a)-(b) above.

(d) Renewal & Documentation. OSIC Personnel must renew their request for certification to collect and report OSINT or review and approve draft OSIRs for release not later than five years after their date of initial certification.

(i) The DUS/C may develop requirements for renewed certification that are different from the requirements for initial certification.

(ii) In the absence of alternative requirements, I&A personnel must fulfill the requirements set forth in Section 3-102-04(a)-(b) above.

(iii) The DUS/C will maintain the authoritative list of OSIC Personnel who have been certified to collect and report OSINT and review and approve draft OSIRs for release.

3-102-05. Open Source Access Plans (OSAPs). Given the wide variety of homeland security-related missions supported by the OSIC Program in a resource-constrained environment, it is especially important that OSIC Personnel prioritize their collection efforts to align to national and departmental intelligence priorities as reflected in I&A's Homeland Intelligence Priorities Framework (IA-HIPF) and Operating Directive, which applies the intelligence prioritization set forth in the IA-HIPF in a collection context. It is also vital that OSIC Personnel demonstrate their fidelity to safeguarding privacy, civil rights, and civil liberties by accessing and reviewing PAI

online in accordance with objective, mission-relevant criteria and not due to any personal prejudice for or against a person’s political, religious, or ideological beliefs. OSIC Personnel satisfy these requirements by developing OSAPs prior to engaging in any collection of online PAI involving First Amendment-protected activities (Protected PAI).

(a) Description. OSAPs are written plans that describe how OSIC Personnel will access and review Protected PAI in a manner that is reasonably calculated to retrieve information responsive to validated collection requirements supporting one or more authorized missions.

(i) [Redacted.]

(ii) [Redacted.]

(iii) OSAPs are written primarily for OSIC Personnel to enable their work without undue administrative burden; however, they should also be written in a manner that facilitates understanding of their contents by internal or external oversight entities unfamiliar with the day-to-day work of the OSIC Program.

(b) Contents. Each OSAP must describe—

(i) The national or departmental mission(s) furthered by the access and review of Protected PAI online, including any relevant intelligence requirements supported by the access and review of that Protected PAI;

(ii) [Redacted.]

(iii) [Redacted.]

(iv) Any measures taken to mitigate the potential for infringing on the privacy, civil rights, or civil liberties of U.S. persons through the unnecessary collection of information about them, which should consider the expected volume and sensitivity of information about U.S. persons likely to be encountered when accessing Protected PAI online.

(c) Issuance and Amendment.

(i) Prior to OSAP issuance, OSIC Personnel will coordinate draft OSAPs with OGC/ILD, TOPO/PIOB, and the Counterintelligence Programs Division within I&A’s Intelligence Enterprise Oversight Program Office (IEPO/CPD) to ensure the intelligence activities contemplated in the OSAPs are legally sufficient, protect individuals’ privacy, civil rights, and civil liberties, and do not give rise to undue counterintelligence concerns.

(ii) Following coordination with OGC/ILD, TOPO/PIOB, and IEPO/CPD, OSIC Personnel submit draft OSAPs to the D/OSID for final approval and issuance.

(iii) Once issued, OSAPs may be supplemented or amended at any time following the process described in Section 3-102-05(c)(i)-(ii) above.

(iv) The OSIC Program and TOPO/PIOB, in coordination with OGC/ILD and, as appropriate, consultation with PRIV and CRCL, will prepare a standardized OSAP template or form that addresses the requirements set forth in Section 3-102-05 above.

(d) Exclusions. OSAPs do not need to address access to, or collection of, the following:

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

(ii) Online sites, platforms, or portals controlled by other federal, foreign, international, state, local tribal, or territorial government entities provided the sites, platforms, or portals are publicly available or widely available to authorized government users, or that such entities authorize I&A access to their sites, platforms, or portals.

3-102-06. Reporting. OSIC Personnel report intelligence and information obtained through their OSINT collection in OSIRs and OSIIs.

(a) [Redacted.]

(b) Protections for U.S. Persons Information.

(i) Notwithstanding the inapplicability of the anonymization requirement in Section 2.3.5 of I&A's Intelligence Oversight Guidelines when disseminating identifying information about U.S. persons (U.S. Persons Information (USPI)) that is PAI, OSIC Personnel will not include USPI in OSIRs or OSIIs.

(ii) OSIC Personnel may provide USPI not included in a disseminated OSIR or OSII as follows:

(A) Generally, OSIC Personnel may provide the USPI in response to a request for such information from a third party where including the USPI would materially assist the third party in using or understanding the OSIR or OSII and the third party provides a valid explanation as to how receipt of the USPI will further one or more of their national or homeland security-related missions.

(B) Consistent with Section 2.3.1 of the Intelligence Oversight Guidelines, OSIC Personnel will only disseminate OSIRs or OSII containing USPI to other that relates to a departmental mission (e.g., domestic violent extremism or the protection of critical infrastructure against domestic threats) to other Intelligence Community elements where they have confirmed the recipient's authority to receive the USPI.

3-102-07. Requests for Assistance.

(a) Focused Collection Requests (FCRs). I&A intelligence personnel outside the OSIC Program may request assistance from the program in collecting and reporting on online PAI through Focused Collection Requests (FCRs) that align to existing or new collection requirements or tactical collection requests on emerging events issued to OSID from IWCC.

(i) FCRs will be processed and reviewed expeditiously by the OSIC Program to determine whether the request can be fulfilled and, if not, why it cannot be fulfilled and whether there are any steps that could be taken to facilitate the collection or an alternative collection.

(ii) Any disagreements over an FCR that cannot be reconciled at the staff level are elevated for resolution, as appropriate.

(b) Requests for Tactical Support. The IWCC, on its own initiative or on behalf of other I&A elements, may request collection and reporting from the OSIC Program for tactical support to all-source reporting on an emerging threat or exigent circumstance. The program will fulfill such requests to the extent practicable given its resources and capabilities.

3-102-08. Temporary Waivers. The DUS/C, to the extent permissible under law, executive order and presidential memorandum, regulation, international agreement and obligation, and national and departmental policy (including I&A's Intelligence Oversight Guidelines), may temporarily waive any provision of Section 3-102-01 through 3-102-07 of this policy guidance where required to respond to exigent threats.

(a) Criteria.

(i) Exigent threats are specific, credible threats arising in the prior 90 days, or reasonably likely to arise in the succeeding 90 days, to the United States, its people, or vital national interests (either domestically or abroad) where the collection of intelligence or information by I&A personnel is reasonably likely to further the efforts of the United States to counter such threats.

(ii) Any temporary waiver, in the assessment of the DUS/C, must be necessary to enable the collection of such intelligence or information (i.e., the collection could not occur otherwise consistent with the provisions of this policy guidance).

(b) Process.

(i) Any OSIC Personnel may request a temporary waiver from the DUS/C through their supervisory chain of command to the D/OSI, who will refer the request to the DUS/C for decision. Non-OSIC Personnel may submit a request for a temporary waiver through their supervisory chain of command to their cognizant Deputy Under Secretary or, for

personnel in the I&A front office, the Chief of Staff, prior to referral to the DUS/C. Alternatively, the DUS/C may pursue a temporary waiver on their own initiative.

(ii) The DUS/C will coordinate any temporary waiver with the Associate General Counsel for Intelligence (AGC/Intel) to ensure the legal sufficiency of any temporary waiver and with the Director of TOPO (D/TOPO) to ensure the protection of privacy, civil rights, and civil liberties in any temporary waiver.

(A) The D/TOPO will consult with PRIV and CRCL on any novel or complex matters pertaining to privacy, civil rights, or civil liberties arising from a proposed temporary waiver.

(B) Any disagreements between the DUS/C and the AGC/Intel or D/TOPO concerning a proposed temporary waiver will be elevated immediately for resolution.

(iii) A temporary waiver may not last beyond the duration of the exigent threat or 90 days, whichever occurs first. If an exigent threat extends beyond 90 days, the DUS/C must request approval of any further extension by the USIA in consultation with the AGC/Intel and D/TOPO.

(iv) The DUS/C will memorialize any temporary waiver, including the exigent threat giving rise to the waiver and why the waiver is necessary to collect intelligence or information reasonably likely to further the efforts of the United States to counter the threat, not later than 30 days from the date of the issuance of the temporary waiver. The DUS/C will provide copies of this memorialization to the AGC/Intel and D/TOPO.

3-103: Geospatial Reporting Program

This section is a placeholder. The policy will be included in a future version of the Policy Manual.

UNCLASSIFIED

PART FOUR: PARTNERSHIPS

UNCLASSIFIED

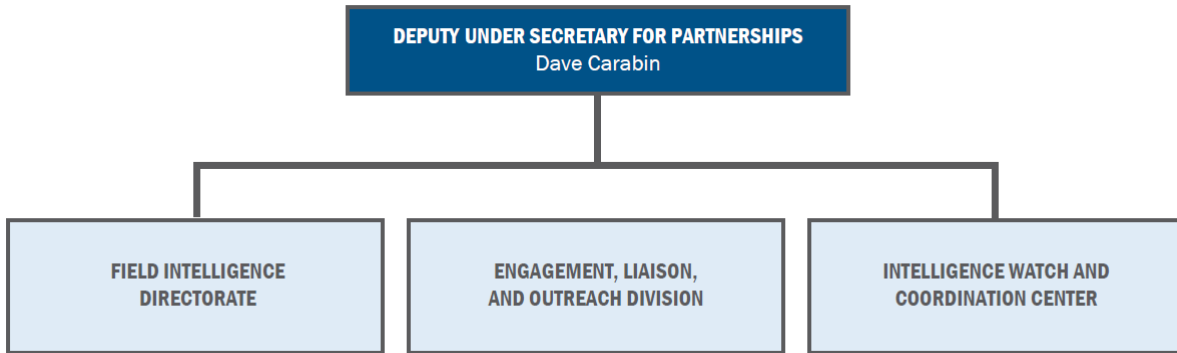
4-101: Organization of the Office of Partnerships

The Office of Partnerships is the lead point of contact within the Office of Intelligence and Analysis (I&A) for its federal, state, local, tribal, territorial, and private sector (FSLTTP) partners, exercising strategic oversight over I&A's external relationships and supervising all I&A officers deployed outside the National Capital Region to support I&A's FSLTTP partners and maintain a strong homeland security intelligence network across the country. The Office of Partnerships is composed of three principal elements: The Engagement, Liaison, and Outreach Division; the Field Intelligence Division; and the Intelligence Watch and Coordination Center.

(a) The Engagement, Liaison, and Outreach Division (ELO). ELO manages strategic relationships with I&A's FSLTTP and international stakeholders. It does this by facilitating multidirectional intelligence and information sharing; assisting partners with their intelligence requirements and needs; enabling partner access to I&A products, resources, and expertise; and advocating on behalf of I&A's partners to advance their homeland security equities within DHS. ELO consists of five branches: the State, Local, Tribal, and Territorial Engagement Branch; the Private Sector Engagement Branch; the National Threat Evaluation & Reporting Branch; the Liaison Officer Branch; and the Foreign Liaison Branch.

(b) The Field Intelligence Directorate (FID). FID comprises field personnel who deliver intelligence to, and develop intelligence from, FSLTTP partners to support operators and decision-makers at all levels of government and the private sector, thereby working to identify and mitigate threats to the homeland. FID executes this mission through a network of approximately 150 officers assigned throughout the country—division directors, division executive officers, division senior intelligence analysts, division collection operations managers, regional directors, and intelligence officers—staffing every one of the 80 fusion centers across the country.

(c) The Intelligence Watch and Coordination Center (IWCC). The IWCC provides 24/7 watch and warning services to the Department of Homeland Security (DHS). It is integrated with the DHS National Operations Center to ensure DHS leaders and operations across the Department maintain situational awareness of homeland security events throughout the United States and around the world. During emerging events, the IWCC produces situational reports that are shared broadly across the homeland security enterprise, including with the Secretary of Homeland Security, the Intelligence Community, and DHS's FSLTTP partners. The IWCC has three branches: the Intelligence Watch Branch, the Intelligence Support Branch, and the Special Events Program Branch. In addition to supporting FSLTTP partners through creation of situational reports, the Intelligence Watch Branch also supports I&A's analytic centers by reviewing ongoing intelligence traffic that meets I&A intelligence requirements. The Intelligence Support Branch manages I&A's request for information program, which allows I&A officers to seek information from FSLTTP partners or for those partners to seek information from I&A. The Special Events Program coordinates federal support to ensure the security of designated events throughout the country.



4-102: Liaison Officer Program

The Liaison Officer (LNO) Program is designed to enhance communication and coordination, and improve the multi-directional flow of information, between the Office of Intelligence and Analysis (I&A) and its federal partners—including Department of Homeland Security (DHS) components and Intelligence Community elements as well as other federal departments and agencies. LNOs play a vital role in sharing information and equipping DHS with the timely intelligence it needs to help keep the homeland safe, secure, and resilient. In addition to supporting the efforts of I&A, LNOs assigned across the federal government support the interactions of their host organizations with DHS components and offices. LNOs are expected to represent I&A and DHS in a professional manner to all levels of leadership.

The LNO Program also encompasses Resident Liaison Officers (RLNOs) assigned to I&A from other interagency partners. RLNOs support the mission of the LNO Program by coordinating and leveraging expertise and information from their parent organizations to share information and enhance visibility, collaboration, and integration of all engagements and initiatives between the parent organization and I&A.

In some circumstances, as approved by the Deputy Under Secretary for Partnerships, the LNO Program will assign an LNO to a host organization due to the special operational needs of I&A or unique requirements and circumstances of the host organization.

(a) LNO Program Objectives. LNOs obtain and maintain access to the proper host organization systems to fulfill responsibilities and conduct activities that support the host organization's interactions with I&A. These activities focus on facilitating the bi-directional flow of information between I&A and the host organization and include—

- (i) Serving as the senior I&A representative to the host organization;
- (ii) Providing subject-matter expertise, advice, and assistance on I&A matters to the host organization;
- (iii) Developing a thorough knowledge of, and building relationships across, the host organization to learn how the host organization can work with I&A and the DHS Intelligence Enterprise;
- (iv) Identifying opportunities within the I&A intelligence production process to include host organization information and opportunities for joint seal productions;
- (v) Educating the host organization about I&A's mission, capabilities, requirements, product lines, systems, tools, and intelligence production processes;
- (vi) Keeping the host organization apprised of I&A activities and priorities and leveraging the host organization's resources and expertise to support I&A mission activities;

(vii) Assisting the host organization and staff with developing intelligence plans and strategies, and creating intelligence opportunities to help counter threats to the homeland; and

(viii) Attending LNO meetings on a routine basis and regularly updating I&A leadership on relevant activities.

(b) Recruiting and Selecting LNO Program Participants.

(i) LNO positions are at the GS-14 and GS-15 grade level. Typically, LNO positions are competed for all I&A personnel, although direct selections can be made to fill positions.

(ii) Individuals must have been employed by I&A for at least two years and received a rating of record of “exceeded expectations” or higher on their most recent performance appraisal before being considered for an LNO position. Applicants provide the materials required by the employment announcement, which generally include, but are not limited to, a resume, cover letter (not to exceed two pages describing qualifications and interest in the position), and performance appraisals accounting for the last two years.

(iii) The LNO Branch Chief conducts interviews consistent with I&A’s internal hiring guidelines, including Recruitment and Selection Board (RSB) processes, and selects qualified candidates to serve as LNOs. The I&A Joint Duty Program Office (JDPO) within the Office of Management's Workforce Management and Engagement Division provides regular updates to applicants for LNO positions regarding their application status.

(iv) After selecting a candidate, the LNO Branch Chief notifies the RSB, JDPO, the selected candidate, and their division or center director. In coordination with the JDPO, the LNO Branch Chief completes a formal Memorandum of Agreement (MOA) with the host organization to establish the terms and conditions of a detail to an LNO position within I&A and assigns the selected individual an LNO position description.

(v) The LNO Branch Chief sends the MOA to the Office of the General Counsel’s Intelligence Law Division for review. Upon successful completion of the legal review, the LNO Branch Chief sends the MOA to the JDPO for final signature and approval by the Deputy Under Secretary for Management (DUS/M) or their designee.

(c) LNO Program Participation and Reintegration.

(i) LNOs adhere to the security requirements of their host organization and notify the LNO Branch Chief of any administrative requirements or personnel actions of the host organization, including, but not limited to, performance plans, time and attendance, or awards.

(ii) Between three and six months prior to the scheduled conclusion of the detail period, the LNO, their I&A supervisor, the LNO Branch Chief, and the JDPO coordinate with

the host organization to determine whether to extend or conclude the detail. The JDPO notifies the LNO of the final determination in writing.

(iii) LNO details generally last two years. An additional one-year extension may be granted with the approval of the Deputy Under Secretary for Partnerships (DUS/P) and host organization. Participants in the LNO Program serve on a non-reimbursable detail and occupy their position of record within the I&A table of organization for the duration of their detail. Upon conclusion of an LNO detail, the employee will return to the position they held prior to acceptance of the LNO detail or to a comparable position.

(iv) LNOs ensure a smooth transition to their successor, including maintaining and transferring continuity materials, explaining and providing details on current projects, introducing the new LNO to key contacts at the host organization, and passing any other information necessary for the new LNO to meet the responsibilities and expectations of the host organization.

(v) At the conclusion of their first detail, an LNO must return to I&A for a minimum of two years prior to applying for another LNO position unless the DUS/M approves an exception.

(d) RLNO Objectives and Oversight.

(i) The DUS/P oversees the receipt and placement of RLNOs based on organizational requirements and consultation with the parent organization.

(ii) RLNOs are expected to adhere to DHS security requirements while serving at I&A.

(iii) The LNO Branch Chief provides support, coordination, and deconfliction, as appropriate, for RLNOs while the parent organization retains responsibility for administrative responsibilities.

(iv) While assigned to I&A, RLNOs are treated as senior representatives of their parent organization and are asked to facilitate intelligence integration across DHS. To succeed in this role, I&A expects RLNOs to improve the information flow between their parent organization and I&A and provide subject matter expertise, advice, and assistance on homeland security matters, including by—

(A) Meeting mutual intelligence needs of DHS and interagency partners;

(B) Integrating their parent organization's efforts into I&A's area of responsibility and DHS's intelligence, operational, and administrative efforts, and helping I&A to understand how the parent organization can support its efforts;

(C) Facilitating the bi-directional flow of information between I&A and their parent organization;

- (D) Assisting I&A with the development of intelligence plans and strategies to create intelligence opportunities to help counter threats to the homeland, and generally supporting intelligence projects and initiatives at I&A;
 - (E) Providing advice, guidance, and intelligence support to I&A leadership and personnel on all applicable matters pertaining to their parent organization's equities; and
 - (F) Attending LNO meetings on a routine basis and regularly updating I&A leadership on relevant activities.
- (v) The continued success of an RLNO is dependent on a smooth transition to their successor at the conclusion of their detail. This includes initiating discussions on extending or concluding the detail with their parent organization supervisor and the I&A LNO branch chief prior to the scheduled conclusion of an RLNO detail.
- (A) I&A will ask the RLNO to maintain and transfer continuity materials, explain and provide details on current projects, introduce the new RLNO to key contacts at I&A, and pass along any other information necessary for the new RLNO to meet their responsibilities and the expectations of I&A before concluding their detail.
 - (B) Upon the conclusion of their detail, the RLNO returns to their parent organization. The LNO Branch Chief works with I&A leadership and the RLNO parent organization to identify a replacement RLNO.
- (e) Non-LNO Program Engagement With LNOs. I&A supervisors may detail I&A personnel who are not participating in the LNO Program to LNO Program host organizations on a full-time, part-time, or *ad hoc* basis under the provisions of Section 5-103 below. Once the detail is approved, per Section 5-103 below, I&A supervisors of the detailed employee notify the JDPO and LNO Branch Chief, who subsequently notify the DUS/P and the LNO assigned to the host organization.

4-103: Notification of Official Travel

This section is a placeholder. The policy will be included in a future version of the Policy Manual.

4-104: Support to Requests for Information

This section is a placeholder. The policy will be included in a future version of the Policy Manual.

4-105: State and Local Security Clearance Requests

Sharing timely, actionable classified information with appropriate cleared state, local, tribal, territorial, and private sector (SLTTP) partners is critical for the protection of the homeland. To maintain this capability, the Office of Intelligence and Analysis (I&A) sponsors clearances for SLTTP partners through the Classified National Security Information Program. This policy guidance provides direction to accelerate and better manage the processing of clearances by delineating criteria for the evaluation of nominations from SLTTP partners.

(a) Eligibility for Sponsorship. I&A sponsors the minimum number of clearances in SLTTP partner entities necessary to support its homeland security missions and only sponsors partners that require classified information to perform their duties.

(i) For I&A to sponsor an SLTTP nominee for a security clearance, the nominee must—

(A) Directly support one or more of I&A’s national or departmental missions as described in I&A’s Intelligence Oversight Guidelines that require a security clearance;

(B) Have a need to know the information to perform their official duties and meet the needs of their organization;

(C) Generally, regularly access facilities and systems approved for processing and sharing information at the requested clearance level⁷;

(D) Commit, to the extent within their control, to actively support the national or departmental mission(s) justifying their clearance nomination for not less than 12 months from the date of receipt of the clearance;

(E) Have been approved by their respective Primary Security Clearance Point of Contact, if applicable; and

(F) Agree to submit to the Department of Homeland Security (DHS) security clearance process, complete all DHS-required training, and abide by relevant DHS policies, including, but not limited to, DHS Directive No. 121-14, *Reporting Requirements for Personnel With Access to Classified Information or Who Hold a Sensitive Position* (as amended June 18, 2024), which implements Security Executive Agent Directive (SEAD) 3, *Reporting Requirements for Personnel With Access to Classified Information or Who Hold a Sensitive Position* (effective June 12, 2017), issued by the Director of National Intelligence. Private sector personnel must also agree to and sign a “Statement of Understanding Relative to the Protection of

⁷ On a limited and case-by-case basis, some SLTTP partners nominated for I&A-sponsored clearances, such as a member of a federally sponsored board, may not be required to have the ability to regularly access facilities and systems approved for processing and sharing information at their appropriate clearance level.

Classified National Security Information” at the time of their read-in as a condition to access classified information.

(ii) I&A ensures that SLTTP nominees meet these criteria by asking nominees a list of curated questions, which nominees must answer for their nominations to be sponsored by I&A. This process does not include the sponsorship of personnel under the purview of Executive Order No. 12,829, *National Industrial Security Program* (as amended Feb. 13, 2015), and the National Industrial Security Program Operating Manual, which is supported directly by the DHS Office of the Chief Security Officer.

(iii) Contractors supporting fusion centers may be eligible for a SECRET-level security clearance. For contractors supporting fusion centers to obtain an I&A-sponsored security clearance, there must be an approved contract and Form DD-254 in place.

(b) Prioritization of Nominations. Eligible nominees for SLTTP security clearances will be prioritized for I&A sponsorship as follows:

(i) *Priority One—State or Territorial Officials*: This category includes governors; homeland security advisors; executive-level law enforcement, homeland security, public safety, and emergency management personnel; and fusion center directors and security liaisons.

(ii) *Priority Two—Local Officials*. This category includes mayors; executive-level fire service and public health personnel; and other senior government officials employed by a city, municipality, county, or other political subdivision of a U.S. state or territory.

(iii) *Priority Three—Other Public Officials*. This category includes all other law enforcement, homeland security, public safety, emergency management, fire service, surface transportation, public health, and emergency response officials participating in a federally sponsored or endorsed board, committee, council, working group, task force, operations center, fusion center, or similar analytic or intelligence entity.

(iv) *Priority Four—Private Sector Officials*. This category includes private sector officials who meet the criteria for eligibility described in Section 4-105(a)(i) above.

(v) *Priority Five—Contractors*. This category includes contractors supporting fusion centers who meet the criteria for eligibility described in Section 4-105(a)(iii) above.

I&A personnel will review the prioritization of nominees monthly to account for any changes in the nominees’ employment or positions within an SLTTP entity.

(c) Clearance Level. Generally, I&A sponsors SLTTP security clearances at the SECRET level; however, I&A may sponsor TOP SECRET (TS)-level security clearances, including Sensitive Compartmented Information (SCI) access, on a case-by-case basis in exceptional circumstances.

(i) I&A will not sponsor a TS//SCI-level clearance absent a demonstrated need such as planned participation in an I&A-sponsored committee, working group, or task force that requires that level of clearance.

(ii) In determining whether to sponsor SLTTP personnel for TS//SCI-level clearances, I&A will give significant weight to the value such a clearance will bring to the effort for which the individual will participate or support.

(d) Sponsorship Determination. I&A's Office of Partnerships is responsible for reviewing SLTTP security clearance nominations and their accompanying justifications to determine whether a nominee meets the eligibility criteria described in Section 4-105(a) above.

(i) Subject to the requirements set forth in Section 4-105(d)(ii)-(iii) below, the Deputy Under Secretary for Partnerships (DUS/P) or their designee makes the final decision whether to sponsor a nomination request.

(ii) The DUS/P or their designee will coordinate their sponsorship decision with the Deputy Assistant Secretary for Intergovernmental Affairs for nominees who are governors, homeland security advisors, mayors, or state cabinet-level positions and with the Executive Director of the DHS Office for State and Local Law Enforcement for nominees who are law enforcement association senior staff.

(iii) Sponsorship for TS//SCI-level clearances must be documented in writing and approved by the DUS/P, or their designee(s).

(e) Terminating Sponsorship.

(i) I&A will terminate its sponsorship for any SLTTP security clearance where the individual holding the clearance no longer meets the eligibility criteria set forth in Section (a) above, including where the clearance holder vacates the position for which the clearance was granted.

(ii) The Office of Partnerships will work with Primary Security Clearance Points of Contact to identify changes in eligibility on an ongoing basis, including by providing these points of contact access to a list of their respective I&A-sponsored security clearances to ensure a continued need for access on the part of the points of contact's respective personnel.

(iii) I&A field personnel will notify the leadership of the Field Intelligence Directorate in the Office of Partnerships of any termination of a sponsorship or changes in an individual's eligibility for sponsorship on a timely basis, but in any event not later than three working days after termination or discovery of the change in eligibility.

4-106: Duty to Warn

If at any time the Office of Intelligence and Analysis (I&A) collects or acquires credible and specific information indicating an impending threat to an intended victim of intentional killing, serious bodily injury, or kidnapping, in compliance with Intelligence Community Directive (ICD) 191, *Duty to Warn* (as amended January 21, 2022), I&A has a duty to warn the intended victim or those responsible for protecting the intended victim by routing the threat information through urgent law enforcement communication channels, as appropriate.

Consistent with the requirements of ICD 191, the director of the directorate, center, or division identifying the threat information serves as the designated senior officer responsible for reviewing threat information initially determined to meet duty to warn requirements to affirm whether the information is sufficiently credible and specific as to permit a meaningful warning.

(a) Threshold Documentation. Issues concerning whether threat information meets the duty to warn threshold are resolved in favor of informing the intended victim if none of the justifications for waiver are met.

(i) The duty to warn process occurs in a timely manner and takes precedence over all other routine matters.

(ii) I&A personnel identifying information they believe relates to an impending threat must pass that information via their chain of command or, in cases of exigent circumstances, directly to the Intelligence Watch and Coordination Center (IWCC).

(iii) The director of the directorate, center, or division identifying the threat information must review the information to determine whether it is sufficiently credible and specific to permit a meaningful warning before asking the IWCC to initiate duty to warn procedures.

(iv) When the information is affirmed and the duty to warn has not been waived, the directorate, center, or division identifying the threat information will document that information and the basis for the duty to warn determination. If necessary and feasible, that directorate, center, or division will prepare an unclassified tearline for use in delivering the threat information to relevant law enforcement officials for investigation and engagement with the intended victim, as appropriate.

(v) Tearlines for delivery to the intended victim via law enforcement channels must not include information that identifies sensitive sources and methods involved in acquiring the information and must be consistent with ICD 209, *Tearline Production and Dissemination* (Sept. 6, 2012).

(vi) If the director of the directorate, center, or division identifying the threat information affirms that the information is credible and specific, but believes that a waiver of the

duty to warn may be appropriate consistent with Section 4-106(f) below, they will brief the information and waiver recommendation to the Principal Deputy Under Secretary for Intelligence and Analysis (PDUSIA). The PDUSIA, in consultation with the Associate General Counsel for Intelligence, will determine whether there is sufficient justification to waive the duty to warn and documents the information and waiver determination.

(b) Communication. Upon determination by the director of the directorate, center, or division identifying the threat information that the information is so credible and specific as to permit a meaningful warning that a duty to warn exists and has not been waived, the communication of threat information to the intended victim via law enforcement can be delivered via eGuardian consistent with any direction provided by the director identifying the threat information.

(i) If the intended victim is in the United States or its territories, the IWCC submits the information via eGuardian for immediate notification to the Federal Bureau of Investigation (FBI) to determine how best to communicate threat information to the intended victim. As appropriate and in partnership with the FBI, I&A leverages communication mechanisms available through the DHS Intelligence Enterprise and federal, state, local, tribal, territorial, and private sector partners.

(ii) If the intended victim is located outside the United States and its territories, the IWCC provides the information to the appropriate Chief of Station through its Intelligence Community watch counterparts to determine how best to communicate threat information to the intended victim. As appropriate and in partnership with the chief of station, I&A leverages communication mechanisms available through Diplomatic Security and the Overseas Advisory Council.

(iii) If the intended victim is a United States Secret Service (USSS) protectee, or the Deputy Secretary of Homeland Security while on overseas travel, the IWCC informs the USSS and the FBI (for intended victims within the United States) or chief of station (for intended victims outside the United States).

(c) Origination of Information. When I&A personnel identify threat information they believe rises to the duty to warn threshold and the information originated with another Intelligence Community element, I&A personnel provide the applicable information to the IWCC. The IWCC notifies the originating element, which determines if a duty to warn exists and, if so, provides the warning and takes any other appropriate action in compliance with ICD 191. The originating element also informs the IWCC of its determination and the course of action taken per ICD 191.

(i) When I&A personnel identify threat information they believe rises to the duty to warn threshold and the information originated with another DHS component or source to

which I&A has unique access, I&A personnel provide the applicable information to the IWCC.

(ii) The IWCC notifies the originating component or source, requesting notification of the originator's intentions and actions regarding the warning. Where the IWCC is notified that the originator does not intend to warn the intended victim, that information is passed to the director of the directorate, center, or division identifying the threat information.

(d) Exigent Threat. When a threat is so imminent as to render consultation or notification impracticable, I&A delivers the threat information to those responsible for protecting the intended victim in an expeditious manner, consulting with the FBI or chief of station to the fullest extent possible. Notification of the delivery of the threat information is made to the FBI or the chief of station, as appropriate, and to the originating element within five days after informing those responsible for protecting the intended victim.

(e) Records. The IWCC documents and maintains records of all duty to warn actions, including, but not limited to—

(i) The method, means, and substance of warning given;

(ii) The senior officer who reviewed the threat information and their determination;

(iii) Any coordination with the FBI or chief of station to provide the threat information and for the FBI or chief of station to determine how best to pass threat information to the intended victim;

(iv) Any coordination with another DHS component, U.S. Government agency, or source regarding delivery of threat information to the intended victim;

(v) Whether the information originated with another DHS component or source to which I&A has unique access and, if so, how and when threat information was delivered to the intended victim and notification of the delivery of that threat information was made to the originating element of the threat information;

(vi) Any decisions to warn the intended victim given exigent circumstances that precluded prior consultation; and

(vii) If the duty to warn is waived, the basis for the waiver.

(f) Waiver. ICD 191 explicitly permits the waiver of a duty to warn and requires Intelligence Community elements' duty to warn procedures to include a provision whereby the duty to warn may be waived. Circumstances where a waiver may be appropriate include the following:

- (i) The intended victim, or those responsible for ensuring the intended victim's safety, already know of the specific threat;
- (ii) The intended victim is at risk only as a result of the intended victim's participation in an insurgency, insurrection, or other armed conflict;
- (iii) There is a reasonable basis for believing that the intended victim is a terrorist, a direct supporter of terrorism, an assassin, a drug trafficker, or involved in violent crimes;
- (iv) Any attempt to warn the intended victim would unduly endanger U.S. Government personnel, sources, methods, intelligence operations, or defense operations;
- (v) The information was acquired from a foreign government with whom the U.S. has formal agreements or liaison relationships, and any attempt to warn the intended victim would unduly endanger the personnel, sources, methods, intelligence operations, or defense operations of that foreign government; or
- (vi) There is no reasonable way to warn the intended victim.

(g) Disputes. Resolution of disputes, both within I&A and among Intelligence Community elements, regarding a determination to warn an intended victim or waive the duty to warn requirement, or regarding the method for communicating the threat information to the intended victim, occurs at the lowest level possible.

- (i) Dispute resolution occurs in a manner that does not unnecessarily delay the timely notification of threat information to the intended victim.
- (ii) Unresolved matters will be elevated expeditiously to the PDUSIA for resolution.

4-107: Nationwide Functional Teams

The management structure within the Office of Intelligence and Analysis (I&A) provides focused supervision of collection, analysis, and partner engagement; nevertheless, there is a need for an integrated management approach across these offices to coordinate and execute the intelligence priorities identified in the I&A Homeland Security Intelligence Priorities Framework (IA-HIPF). I&A's activities in the field are multidimensional. Field officers both manage relationships with federal, state, local, tribal, territorial, and private sector (FSLTTP) entities and perform collection and analytic functions. Integrated management allows for direction on matters of tradecraft and standards from the Deputy Under Secretary for Collection (DUS/C) and the Deputy Under Secretary for Analysis (DUS/A) while recognizing that the responsibility to directly manage and provide meaningful oversight to field officers is most effectively carried out by the Deputy Under Secretary for Partnerships (DUS/P) and leadership in the Field Intelligence Directorate (FID), which reports to the DUS/P.

To facilitate this integrated management approach in an effective and streamlined manner, the DUS/A, DUS/P, and DUS/C have developed Nationwide Functional Teams to synchronize efforts between the field and I&A headquarters through the use of joint Analysis, Collection, and Engagement (ACE) plans—ensuring that I&A works in unison to counter the most pressing homeland security threats. This guidance memorandum formalizes the structure and processes of the NFTs to enable coordination across I&A's operations. It does not alter the responsibilities of the DUS/A, DUS/P, or DUS/C with respect to their control of personnel, budgets, or unique operations.

4-107-01. NFT Composition.

I&A maintains one NFT aligned to each analytic center.

(a) Membership.

(i) Each NFT includes the following core members:

(A) A single NFT Program Coordinator (NPC), who is a FID officer reporting through the FID chain of command, serves as the overall project manager for the NFT, including by—

(I) Coordinating with Partnerships, Analysis, and Collection personnel to enable collaboration on identified intelligence priorities;

(II) Leading the development and implementation of ACE plans and engagement materials; and

(III) Overseeing NFT processes and programs, organizing meetings, nominating IA-HIPF subtopics, and archiving engagement materials where they can be accessed by I&A field personnel;

(B) A Division Senior Intelligence Analyst, who leads the development of “finished” analytic products identified in ACE plans, including by—

(I) Identifying finished analytic production opportunities and reviewing draft analytic products that align to their assigned NFT;

(II) Coordinating production planning and draft analytic products with their respective NPC and analytic center;

(III) Supporting the production of engagement materials such as slide decks and talking points, “Regional Perspectives” documents, tearlines, and downgraded products for FSLTTP engagement; and

(IV) Supporting other NFTs, among other ways, by identifying analytic opportunities within their division to execute the goals outlined by the NFT while aligning the division’s equities and inputs to analytic requirements; and

(C) A Division Collection Operations Manager (DCOM) to lead the development of the FID collection portions of NFT plans, including by—

(I) Identifying collection opportunities within their division and aligning the division’s equities and inputs to collection requirements;

(II) Identifying partners for liaison exchanges and working with the Collection Management Division (CMD) to identify specific collection gaps based on input received from the analytic centers;

(III) Ensuring field personnel have materials for collection-focused engagements, such as slide decks incorporating technical or substantive information from Collection Support Primers and other guidance from the Operating Directive (OD);

(IV) Reviewing and coordinating Operational Proposals for proposed field interviews; and

(V) Maintaining visibility into Source Directed Requirements (SDRs) (i.e., specific requests or taskings for a collector to question a contact on a particular collection requirement) and Requests for Information across all offices on their assigned functional topic.

(ii) In addition, NFTs receive dedicated support from the following officials:

(A) At least one experienced senior analyst or manager from the analytic center aligned to the NFT who can speak to the full range of analytic portfolios and production plans throughout the center, who has the authority to represent the center’s equities, and who serves as the center’s analytic liaison to the NFT, including by—

- (I) Producing relevant analytic products and judgments on identified intelligence priorities and evaluating I&A's field and open source reporting;
 - (II) Sharing information on analytic portfolios, production plans, and key intelligence questions;
 - (III) Developing ACE plan engagement materials, slide decks, and talking points;
 - (IV) Helping to ensure the analysts within their respective analytic center assist with the identification of the IA-HIPF sub-topics that will be a priority for the NFT;
 - (V) Providing subject matter expertise to CMD to review, develop, or update requirements to drive collection and reporting efforts; and
 - (VI) Participating in Weekly I&A Field Intelligence, Monthly I&A/SLTT Intelligence exchanges, and other synchronization meetings;
- (B) A single collection requirements manager assigned by CMD to support each NFT, including by—
- (I) Working with analysts to review, develop, update, and validate collection requirements;
 - (II) Helping to align Operational Directive and NFT priorities;
 - (III) Supporting the NPC and DCOM in developing the collection portions of NFT plans, including any supporting materials such as Collection Support Primers and Notices of Intelligence Potential; and
 - (IV) Ensuring analysts receive and evaluate FID and Open Source Intelligence Division (OSID) serialized, unevaluated ("raw") intelligence reporting and submit SDRs against relevant FID reporting to drive further collection;
- (C) A primary regional representative (and alternate representative), selected by the cognizant Regional Director, from each of I&A's 10 field regions, who serves as the touchpoint between the NFT and their respective FID region, helping to ensure that NFT projects account for the capabilities and opportunities within each region and that each regional team is aware of NFT priorities and ACE plans; and
- (D) An OSID collector assigned to each NFT to advise on relevant open source collection, aligned to existing collection requirements, that may help inform the NFT.
- (iii) Each NFT may include additional participants such as non-primary representatives from the FID regions or analytic centers, officers from the Homeland Identity Intelligence Center (HI2C) or the Intelligence Watch and Coordination Center, or non-I&A personnel such as FSLTTP partners. The NPC, subject to any guidance or direction

provided by the governing board for their respective NFT consistent with Section 4-107-01(b) below, will determine the final membership for their respective NFT.

(iv) With the exception of the NPC, all core and support officials assist the NFT as a collateral duty. Assistance includes, but is not limited to, developing NFT priorities and ACE plans, attending NFT meetings and contributing constructive input, maintaining threat awareness of the analytic storyline, briefing engagement materials, creating Notices of Intelligence Potential, drafting regional perspectives, fostering robust FSLTTP relationships, and seeking new ones based on the threat topic. Should an NFT member not actively participate in or support the NFT, the NPC will report this to the FID Deputy Director for Engagement, who will coordinate with the appropriate governing board cochair for follow-on action.

(b) Governing Board. Each NFT is led by a governing board, which is cochaired by a division director within FID, the director or deputy director of the analytic center aligned to the NFT, and the Director or Deputy Director of CMD.

(i) The cochairs ensure that the personnel, processes, and resources within Partnerships, Analysis, and Collection are appropriately aligned to execute the goals established by the NFT, including by validating IA-HIPF nominations and ACE plans.

(ii) Personnel serving on the governing board must have at least one annual performance goal covering support for the NFT.

4-107-02. NFT Activities.

NFTs identify IA-HIPF sub-topics that are a near term focus for I&A's analytic centers and FSLTTP partners, including the broader Intelligence Community. In coordination with FID, NFTs engage with FSLTTP partners and OSID to collect and report information that addresses validated intelligence gaps aligned to those sub-topics. NFTs also coordinate intelligence production between the analytic centers and FID and develop briefing materials to share with FSLTTP partners.

(a) Identification of NFT Priorities. Every six months, each NFT proposes no more than two IA-HIPF sub-topics that will be a priority for Analysis, Collection, and Partnerships. The goal is to identify sub-topics for which no other department or agency provides intelligence support or topics or where I&A makes unique contributions distinct from the work of other departments and agencies.

(i) The NFT considers I&A's capability to address potential sub-topics through analysis, collection, and partner engagement (including by incorporating SLTTP intelligence priorities that align with our homeland security missions), prioritizing topics designated as "tier one" topics in the IA-HIPF, the Operating Directive, and the Program of Analysis. Ascertaining that capability might require surveying relevant personnel and reviewing regional collection posture statements, domain threat assessments, and production plans.

(ii) Each NFT's priority topics must be approved by the DUS/A, DUS/P, and DUS/C before the NFT may act on them.

(b) ACE Plans. To focus I&A's work on the NFT's priorities, each NFT must develop and maintain at least one active ACE plan. ACE plans provide direction from an NFT to the relevant personnel within Analysis, Collection, and Partnerships consistent with the requirements set forth below.

(i) *Goals*. Each ACE plan outlines goals and desired outcomes, which may include the following:

(A) Ensuring key partners across the Nation have the information they need about a particular homeland security threat or vulnerability to make appropriate policy, operational, and enforcement decisions (information sharing);

(B) Producing raw intelligence reports to provide a nationwide picture of a given threat sub-topic (collection); and

(C) Supplementing finished analytic products to advance national or regional understanding of a particular homeland security threat or vulnerability (analysis).

(ii) *Taskings*. ACE plans will direct information sharing, collection, and analysis for the NFT through written taskings, which must be clear and quantifiable.

(A) For example, an ACE plan can direct a region to conduct outreach to multiple partners within a specific sector, with a particular title, or within certain organizations. An ACE plan can similarly direct a region to produce a specified number of raw intelligence reports or finished analytic products.

(B) The plan can also inform priorities and suggest activities for headquarters elements such as analytic centers, CMD, the OSID, or HI2C.

(iii) *Performance Measures*. Each ACE plan will include criteria for assessing the success of the plan. These criteria will include specific, measurable, and objective metrics—such as the number of intelligence reports, analytic products, and briefings conducted pursuant to the plan—and contextual indicators of success, such as operational and broader policy or decisional impact.

(iv) *Supporting Materials*. ACE plans will include engagement materials such as briefing decks, talking points, and other supporting documents to equip field personnel with necessary information. Engagement materials will be released concurrent with the plans.

(v) *Duration*. NFTs must review each ACE plan at least once every 90 days to break down longer term projects into manageable sub-tasks that can be completed within this timeframe.

(vi) *Approval.* An ACE plan is approved upon signature by the governing board for the NFT described in Section 4-107-01(b) and the FID Director.

(vii) *ACE Plan Execution Updates.* Not later than 90 days after approval of an NFT's ACE plan and every 90 days thereafter until completion of the plan, the NPC, in coordination with the NFT's governing board cochairs, will brief the DUS/A, DUS/P, and DUS/C on the implementation of the plan with input from the cognizant regional director and appropriate headquarters personnel. This update will characterize the performance of each region and relevant headquarters divisions.

4-201: Field Intelligence Program

The Office of Intelligence and Analysis (I&A) supports the intelligence and information needs of the Department of Homeland Security (DHS) and its federal, state, local, tribal, territorial, and private sector (FSLTTP) partners through the collection of intelligence and information overtly or from publicly available sources. The primary means by which I&A accomplishes the former mode of collection is through liaison exchanges and, less frequently, field interviews. Collectively, these activities comprise the Field Intelligence Program (FIP).

I&A holds itself to the highest standards of conduct when it comes to the tradecraft with which it executes its national and departmental missions. Unlike other overt collection programs within the Intelligence Community such as that conducted by the Department of Defense, I&A is not well postured to run sources or apply clandestine tradecraft. Given its homeland focus, I&A also has a special responsibility to ensure that its intelligence activities comply with the Constitution and the laws of the United States and protect individuals' privacy, civil rights, and civil liberties. I&A therefore carefully applies its unique overt tradecraft in accordance with its authorities and restrictions to collect information of intelligence value to the Intelligence Community and to FSLTTP partners.

The FIP provides I&A personnel with the flexibility they need to gather information that helps protect against threats to homeland security. The program addresses every aspect of a functioning, mature overt collection function—from certification to operational planning, to contact memorialization. I&A personnel participating in the FIP are expected to comply with the requirements and restrictions set forth in this policy guidance at all times.

4-201-01. Scope and Focus.

(a) Activities Within the FIP. The FIP encompasses the overt collection of intelligence and information by intelligence personnel in the Field Intelligence Directorate (FIP Personnel) through liaison exchanges or field interviews. It does not include the collection of intelligence or information from open sources, which is addressed through policies, processes, and standards applicable to the Open Source Intelligence Collection (OSIC) Program, or collection in support of investigative or operational efforts to counter espionage and other foreign intelligence activities against the Department, which is conducted by I&A's Counterintelligence Program. It also does not include, and this memorandum does not apply to, the receipt by I&A of newspapers or other periodicals; books, journal articles, or other published works or reports; public filings or records; or similar documents or databases, whether accessed through a subscription or accessible free of cost.

(i) I&A uses the term "liaison exchange" to encompass the solicitation and collection of information from employees or contractors of foreign, state, local, tribal, or territorial governments (or any agency or subdivision thereof); the private sector; or other elements of the federal government (including DHS components) when those individuals are acting in a representational capacity on behalf of their employers (i.e., as liaisons).

Liaison exchanges do not include interactions between I&A personnel and liaisons for purposes other than the collection of information or intelligence for serialization in raw intelligence reports or other intelligence purposes.

(ii) The term “field interview” refers to the solicitation of information from non-liaison individuals or liaison personnel who are not speaking in a representational capacity for their employer or contracting entity, including interviews of liaison personnel in their personal (as opposed to official or representational) capacity.

(iii) When an encounter with an individual reasonably could be categorized as either a liaison exchange or a field interview, the encounter is handled as a field interview.

(b) Focus of the FIP. The primary focus of the FIP is on liaison exchanges, with field interviews limited in most circumstances to individuals in U.S. Customs and Border Protection (CBP) or U.S. Immigration and Customs Enforcement (ICE) administrative detention (i.e., CBP temporary custody at a port of entry or ICE custody at an immigration detention facility, or otherwise in the custody or under the control of CBP or ICE).

(i) These field interviews will focus on intelligence and information pertaining to border security (including maritime border security), transnational organized crime, and terrorism.

(ii) I&A personnel, on a case-by-case basis, may conduct one-time field interviews outside the administrative detention context where an opportunity presents itself to obtain and report intelligence or information concerning national or homeland security threats or vulnerabilities that is appropriate for Intelligence Community, departmental, or FSLTTP audiences, but would not otherwise be reported to those audiences.

(A) I&A personnel must confirm that other relevant federal Intelligence Community and law enforcement partners are unwilling or unable to report such intelligence or information before pursuing a field interview outside the administrative detention context.

(B) Where such circumstances exist and I&A personnel wish to conduct a field interview, they still must comply with the requirements set forth in Sections 4-201-01 through 4-201-04 and 4-201-06 through 4-201-07 below, including the requirement to submit an operational proposal for review prior to conducting the interview.

(C) I&A personnel may interview individuals in DHS administrative detention more than once while such individuals are in administrative detention.

(iii) All other potential field contacts should be referred to FSLTT intelligence or law enforcement partners for action, with any relevant information obtained by those partners collected by I&A via liaison exchange with that partner.

(c) Authorized Personnel. Only FIP Personnel may conduct liaison exchanges or field interviews within the scope of the FIP.

(d) Sources and Contacts. I&A currently lacks the resources and infrastructure to validate and manage sources on an ongoing basis in a manner that is effective and consistent with Intelligence Community standards.

(i) Where FIP Personnel encounter a field contact who is reasonably believed to possess intelligence or information, or access to intelligence or information, that makes them a viable candidate for persistent contact with the Intelligence Community or an FSLTT law enforcement agency as an intelligence or law enforcement source, I&A will refer that potential source to the appropriate Intelligence Community element or FSLTT law enforcement agency with the jurisdiction, mission, resources, and capabilities to maintain contact with the potential source.

(ii) Where helpful to the relationship with, or usefulness of, the potential source to the Intelligence Community element or FSLTT law enforcement agency receiving a referral from I&A, FIP Personnel may provide additional assistance in the form of joint source handling where permitted by the Intelligence Community element or FSLTT law enforcement agency and the joint source handling is conducted in accordance with all applicable policies, practices, and procedures, including the other requirements, restrictions, and safeguards set forth in this policy guidance.

(A) I&A joint source handling with another Intelligence Community element or FSLTT law enforcement agency must be conducted consistent with, and may not commence until DUS/C and DUS/P issue, standard operating procedures that provide further guidance about the documentation and oversight requirements for this type of joint activity.

(B) I&A personnel are still bound by all other provisions of this guidance when partnering with an Intelligence Community element or FSLTT law enforcement agency.

(iii) This restriction on source management is not intended, and should not be interpreted or applied, to prevent FIP Personnel from interviewing individuals in DHS administrative detention more than once while such individuals are in administrative detention consistent with Section 4-201-01(b)(ii)(C) above.

4-201-02. General Requirements. Liaison exchanges and field interviews are different activities with different purposes, methods, and implications for privacy, civil rights, and civil liberties. Nevertheless, there are some requirements that apply to both activities.

(a) Compliance With Intelligence Oversight Guidelines. FIP Personnel, like all I&A personnel, are required to follow I&A's Intelligence Oversight Guidelines when engaging in intelligence activities. This includes, but is not limited to, the following:

(i) Under I&A's Intelligence Oversight Guidelines, the acquisition of any information from outside the Intelligence Community for intelligence purposes constitutes collection. Accordingly, any acquisition of information outside the Intelligence Community through a liaison exchange or field interview must be overt or from publicly available sources.

(ii) FIP Personnel are prohibited from engaging in any intelligence activity for the purpose of affecting the political process in the United States, for the sole purpose of monitoring activities protected by the First Amendment or the lawful exercise of other rights secured by the Constitution or laws of the United States, or for the purpose of retaliating against a whistleblower or suppressing or burdening criticism or dissent.

(iii) FIP Personnel are prohibited from engaging in intelligence activities based solely on an individual's or group's race, ethnicity, gender, gender identity, religion, sexual orientation, gender, gender identity, country of birth, nationality, or disability. The use of these characteristics is permitted only in combination with other information, and only where such use (1) is intended and reasonably believed to support one or more of I&A's national or departmental missions and (2) is narrowly focused in support of that mission (or those missions).

(iv) FIP Personnel must reasonably believe that any intelligence activity furthers one or more of I&A's national or departmental missions to conduct them.

(v) FIP Personnel are prohibited from engaging in physical surveillance.

(vi) FIP Personnel may not request or direct any other person or entity, including liaison partners, to engage in any conduct prohibited by the Constitution, applicable laws, or Executive Order No. 12,333.

(b) Prohibition on Targeting Journalists. FIP Personnel are prohibited from engaging in any collection targeting journalists in the performance of their journalistic functions.

(i) This prohibition applies to any individual gathering or editing news for presentation through any media regardless of whether the individual is employed by or acting on behalf of an accredited, certified, or otherwise professionally recognized media provider.

(ii) The prohibition applies to journalists when they are engaging in journalistic functions. Journalists engaging in non-journalistic activities, including any activity that violates federal criminal law, may be targeted for collection of intelligence or information concerning those non-journalistic activities to the extent such collection furthers a national or departmental mission and otherwise is permissible under I&A's Intelligence Oversight Guidelines and other applicable policies and procedures, including this policy guidance.

(iii) The prohibition applies to any collection of intelligence and information where a journalist's journalistic activities are the target or subject of the collection. It does not prohibit I&A from collecting intelligence or information from a journalist (or news organization), or publicly available information authored by and otherwise attributable to a named journalist, so long as the target of the collection is not a journalist engaging in journalistic functions.

(c) Tasking Collection. Tasking is either directly or indirectly demanding or directing contacts to collect, or requesting that contacts collect, intelligence or information on behalf of I&A that is not already in their possession.

(i) FIP Personnel are prohibited from tasking any contact outside the Intelligence Community to collect intelligence or information on behalf of I&A absent prior coordination with the DHS Office of the General Counsel's Intelligence Law Division (OGC/ILD) and the Privacy and Intelligence Oversight Branch within I&A's Transparency and Oversight Program Office (TOPO/PIOB).

(ii) FIP Personnel may ask liaison contacts to provide information that is already in their possession and meets Intelligence Community or departmental collection requirements. They also may provide intelligence priorities and collection requirements to liaison contacts so long as FIP Personnel do not request that liaison contacts engage in behavior on behalf of I&A that would be impermissible for I&A personnel.

(d) Communication Devices and Platforms. When engaging in their official duties, FIP Personnel may only use communication devices or platforms (e.g., messaging applications) that are provided by, or explicitly authorized for use by, DHS for official duties.

(e) Personal Relationships with Contacts. FIP Personnel may not undertake any act in their official capacity for the benefit of, or to the detriment to, a third party for personal reasons, nor may they treat any third party differently from other similarly situated third parties based on their personal relationship with, or personal feelings toward, that third party.

(f) Prohibition on Coercion and Unlawful Acts. FIP Personnel may not, under any circumstances, coerce, threaten, or intimidate a contact, whether directly or indirectly (e.g., intimidating a contact through deception or implication), nor may they engage in any activity

in violation of the laws of the United States, including the laws of any state, territory, or subdivision thereof.

4-201-03. Certification. The starting point for participation in the FIP is program certification. The certifications required for FIP Personnel vary depending on whether they seek to engage only in liaison exchanges or also in field interviews.

(a) Certification for Liaison Exchanges. To be certified as eligible to conduct liaison exchanges, FIP Personnel must complete training developed or endorsed by I&A that enables them to conduct and document liaison exchanges consistent with applicable overt tradecraft, including by producing raw intelligence reports for appropriate audiences. FIP Personnel must also complete their required intelligence oversight training consistent with I&A's Intelligence Oversight Guidelines.

(i) Previously, this training was delivered through the Reports Officer Course (ROC); per the direction of the USIA, this training is being evaluated for potential revision or replacement. Following their review of the ROC, the DUS/C, in consultation with the DUS/P and Deputy Under Secretary for Management (DUS/M) in their role overseeing training to I&A personnel, will determine whether the ROC, either as it currently exists or as revised, or a replacement course, satisfies the requirements set forth in 4-201-03(a) above.

(A) Until such time as the ROC is revised or replaced, FIP Personnel are deemed to have satisfied the training required by 4-201-03(a) above through successful completion of the ROC.

(B) As the ROC is revised or replaced, FIP Personnel must complete the revised or new training within one year of the availability of the revised or new training.

(C) The DUS/C or DUS/P, in consultation with each other, may extend the training deadline set forth in Section 4-201-03(a)(i)(B) above.

(ii) Upon fulfilling their training requirements, FIP Personnel submit a request for certification to conduct liaison exchanges to their supervisors along with confirmation from the Intelligence Training Academy (ITA) that they have completed their required training, including intelligence oversight training. Their supervisors submit these materials through their chain of command to the Director of the Field Intelligence Directorate (FID), who submits the request along with their recommendation on certification for decision by the DUS/C and the DUS/P.

(iii) FIP Personnel may not draft any serialized raw intelligence reports arising from liaison exchanges unless and until they are certified as eligible to conduct liaison exchanges by the DUS/C and the DUS/P.

(b) Additional Certification for Field Interviews. To be certified as eligible to conduct field interviews in addition to liaison exchanges, FIP Personnel, in addition to the requirements set forth in Section 4-201-03(a) above, must occupy a position within FID designated to collect intelligence or information through field interviews and complete specific training on field interviews developed or endorsed by I&A.

(i) Previously, this training was delivered through the Overt Collection Course (OCC); this training is being evaluated by the DUS/C, in consultation with the DUS/P and DUS/M, in their respective roles overseeing and administering training to I&A personnel, for potential revision or replacement. Following their review of the OCC, the DUS/C will determine whether the OCC, either in its current or a revised form, or a replacement course, satisfies the requirements set forth in Section 4-201-03(b) above.

(A) Until such time as the OCC is replaced or revised, FIP Personnel are deemed to have satisfied the training required by Section 4-201-03(b) above through successful completion of the OCC.

(B) As the OCC is revised or replaced, FIP Personnel must complete the revised or new training within one year of the availability of the revised or new training.

(C) The DUS/C or DUS/P, in consultation with each other, may extend the training deadline set forth in Section 4-201-03(b)(i)(B) above.

(ii) Upon fulfilling these requirements, FIP Personnel submit a request for certification to conduct field interviews along with certification from the ITA that they have completed their required training. Their supervisors submit these materials through their chain of command to the Director of FID and Director of the Collection Management Division, who submit the request along with their joint recommendation on certification for decision by the DUS/C and DUS/P.

(iii) FIP Personnel may not engage in field interviews unless and until they are certified to conduct field interviews by the DUS/C and DUS/P.

(c) Provisional Certification. In those rare circumstances where strict compliance with the requirements described in Section 4-201-03(a)-(b) above would materially impair I&A's capability to collect or report intelligence or information in furtherance of I&A's national or departmental missions, the DUS/C, with the DUS/P, may provisionally certify I&A intelligence personnel who meet the requirements for certification other than those pertaining to training where the personnel, in the judgment of the DUS/C and DUS/P, have received equivalent training or developed sufficient experience such that they can perform liaison exchanges or field interviews at the same level of proficiency as fully trained personnel. To the greatest extent practicable, provisionally certified personnel will be assigned to supervisory or managerial FIP Personnel who have received the required training.

(i) Provisional certification must be memorialized by the DUS/C to go into effect and will remain effective for not more than one year from the date of provisional certification.

(ii) Personnel can only be provisionally certified once; thereafter, they must satisfy all requirements set forth in Section 4-201-03(a)-(b) above to retain their certification.

(iii) Under no circumstances may the DUS/C or DUS/P provisionally certify I&A intelligence personnel to engage in field interviews where those personnel have not completed the intelligence oversight training required under Section 4-201-03(a)-(b) above.

(d) Renewal & Documentation. FIP Personnel must renew their request for certification to conduct liaison exchanges or field interviews not later than five years after their date of initial certification.

(i) The DUS/C, with the DUS/P, may develop requirements for renewed certification that are different from the requirements for initial certification.

(ii) In the absence of alternative requirements, I&A personnel must fulfill the requirements set forth in Section 4-201-03(a)-(b) above.

(iii) The DUS/C will maintain the authoritative list of FIP Personnel who have been certified to conduct liaison collection and field interviews.

4-201-04. Operational Proposals (OPSPROs). Field interviews, and some liaison exchanges, present comparatively higher risks from an operational, counterintelligence, legal, privacy, civil rights, or civil liberties perspective. To address these heightened risks, FIP Personnel must submit and receive approval of OPSPROs under the circumstances, and consistent with the requirements, set forth below.

(a) Applicability. OPSPROs are required under the following circumstances:

(i) OPSPROs are required for field interviews, including field interviews of individuals in DHS administrative detention. They are not required for information that is provided by field contacts without prompting by, or a request from, I&A.

(ii) OPSPROs are also required for liaison exchanges that give rise to special concerns about the risks such exchanges may pose to the FIP Personnel or partners engaging in them, including the following:

(A) Liaison exchanges where the interaction with the liaison contact is recorded by video or audio except where the host organization records interactions with contacts as a matter of policy or practice;

(B) Liaison exchanges arising from the attendance of I&A personnel at a conference or group meeting in their professional capacity and for the purpose of collecting intelligence or information for reporting (i.e., not where I&A personnel attend a conference or group meeting for general engagement with FSLTTP partners);

(C) Liaison exchanges with individuals who are—

(I) Employed by a foreign government or international organization (or any agency or subdivision thereof);

(II) Members of the clergy;

(III) Journalists or media representatives;

(IV) Health care providers (including mental health providers) when discussing specific patients;

(V) Attorneys about a matter in which they represent a party;

(VI) Employees of, or volunteers representing, non-governmental organizations engaging in humanitarian relief efforts; or

(VII) Refugees, asylees or asylum-seekers, or individuals seeking or receiving T visas, U visas, or an immigration benefit under the Violence Against Women Act of 1994; or

(D) Liaison exchanges with any other categories of individuals jointly identified by the DUS/C and DUS/P, in consultation with the Associate General Counsel for Intelligence (AGC/Intel) and the Director of the Transparency and Oversight Program Office (D/TOPO), as giving rise to the concerns described above.

(iii) The DUS/C and DUS/P may jointly require an OPSPRO for any other liaison exchange in addition to those requiring an OPSPRO under Section 4-201-04(a)(ii) above.

(b) Scope. Generally, open-ended OPSPROs will not be approved; however, individual OPSPROs may cover more than one interview within a specifically defined timeframe, duration, or location so long as the OPSPRO describes the type(s) of interviews to be conducted (e.g., they may cover a specified program of interviews).

(i) For example, an OPSPRO covering a multi-week deployment to a specific area at the U.S. border to interview individuals who lack authorization to enter the country and are reasonably likely to possess information concerning transnational criminal organizations encountered at the border by CBP would be an appropriately scoped OPSPRO.

(ii) In contrast, an OPSPRO seeking permission to interview any individual in the administrative detention of CBP anywhere in the United States over the course of the following year would not.

(c) Requirements. Each OPSPRO must be—

(i) Tailored to a defined and planned collection event or series of events, providing—

(A) The specific time(s) (or range of times) and location(s) for the intended collection;

(B) The collector(s), by name;

(C) The information intended to be collected, including the essential elements of information within an identified collection requirement (or requirements) to be collected and how the collection requirement aligns with the prioritization of collection requirements set forth in the I&A Operating Directive;

(D) Information about the intended contact(s) and the circumstances surrounding the intended liaison exchange or field interview, including detailed information regarding the circumstances of a contact's custodial status, if applicable;

(E) For proposed field interviews—

(I) Whether potential field contacts are in law enforcement or DHS administrative custody, or have been criminally charged or arraigned (and, if so, whether their guilt with respect to such matters has been fully adjudicated (including sentencing)) along with the efforts already, or to be, taken to determine whether the potential field contacts fall within any of the categories described in Section 4-201-04(a)(ii)(C) above; and

(II) If the proposed field interview is outside the administrative detention context, whether other relevant Intelligence Community and federal law enforcement partners are unwilling or unable to report such intelligence or information along with the justification for this determination;

(F) Any law enforcement agencies whose officials are attending the liaison exchanges or field interviews, and, if so, whether those officials intend to record any interactions with the contact (and, if so, why), or, if no law enforcement agencies will have officials in attendance, why they are absent;

(G) Any items of monetary value to be provided to the contact(s) other than *de minimis* amounts of basic items such as food, water, or tobacco items; and

- (H) An intelligence gain/loss assessment;
 - (ii) Responsive to a valid, identified Intelligence Community or departmental collection requirement;
 - (iii) Approved by the regional and division directors overseeing the division(s) and region(s) in which the collection would take place; and
 - (iv) Approved by the DUS/C and DUS/P following consultation with the Executive Director of the Intelligence Enterprise Program Office (ED/IEPO), the D/TOPO, and the AGC/Intel through a Senior Review Panel convened to review and discuss the OPSPRO.
- (d) Reviews.
- (i) The following factors will be considered in the review of OPSPROs:
 - (A) The value of the information reasonably expected from the contact;
 - (B) The likelihood that the contact can provide the desired information;
 - (C) Operational and counterintelligence risks;
 - (D) The likely impact of the proposed liaison exchange or field interview on individuals' privacy, civil rights, and civil liberties;
 - (E) The likelihood that the proposed liaison exchange or field interview will result in serialized reporting on topics or subjects that otherwise would not be captured by DHS component or Intelligence Community serialized reporting; and
 - (F) The availability of the desired information through lower risk means.
 - (ii) Absent extenuating circumstances or the need for additional information, the initial review of OPSPROs by the I&A officials named in Section 4-201-04(c)(iii)-(iv) above will be completed no later than five working days from their receipt of the OPSPRO.
 - (A) FIP Personnel should notify the officials named in Section 4-201-04(c)(iii)-(iv) above when extenuating circumstances require expedited review of an OPSPRO.
 - (B) For OPSPROs involving novel or unusually complex circumstances, FIP Personnel are encouraged to develop their OPSPROs in consultation with the officials named in Section 4-201-04(c)(iii)-(iv) above to facilitate timely review and approval.

4-201-05. Conducting Liaison Exchanges. Liaison exchanges are subject to I&A's Intelligence Oversight Guidelines, meaning that FIP Personnel must comply with the Guidelines'

requirements and restrictions concerning access to, and collection and retention of, liaison contact information. Liaison contacts, however, should not be subjected to the same intelligence tactics, techniques, or procedures that might be applied in the context of a field interview.

(a) Transparency. FIP Personnel must be transparent with liaison contacts about their identity, affiliation with I&A, responsibilities within the FIP, and their intent to use any intelligence or information provided or made available to them by liaison contacts for intelligence purposes such as analysis or dissemination. To the extent relevant, FIP Personnel must also inform liaison contacts of the requirements and restrictions on FIP Personnel arising from I&A's Intelligence Oversight Guidelines and this memorandum.

(b) Collection and Use of Personally Identifiable Information (PII). FIP Personnel take appropriate measures to limit the collection and use of PII concerning liaison contacts.

(i) For SLTT partners, FIP Personnel should not collect more PII than a liaison contact's name, position and organizational affiliation, and professional contact information. This information is collected solely to verify the contact's identity and for recall purposes, and it will not be used to coordinate, deconflict, or register the field contacts with Intelligence Community, departmental, or law enforcement partners.

(ii) For employees or contractors of foreign governments or private sector individuals, FIP Personnel may obtain additional PII or other data necessary not only to verify the contact's identity and for recall purposes, but also to coordinate, deconflict, and register the field contacts with relevant Intelligence Community, departmental, and law enforcement partners.

(iii) FIP Personnel also may conduct research from publicly available sources about liaison contacts to understand their professional background, expertise, or ability to provide information via liaison exchange that is responsive to Intelligence Community or departmental collection requirements.

4-201-06. Conducting Field Interviews. While most information received by I&A employees deployed to the field comes through liaison exchanges, I&A's field interviews of individuals in a non-representational capacity, conducted on an overt and voluntary basis, provide an important conduit of information that helps to ensure the timely delivery of intelligence to homeland security stakeholders. Field interviews differ from liaison exchanges with respect to their operational; legal; privacy, civil rights, and civil liberties; and counterintelligence implications. Therefore, they operate under different rules as set forth below.

(a) Preliminary Engagements With Potential Field Contacts and Referral Checks.

(i) Prior to requesting approval of an OPSPRO to conduct a field interview outside the administrative detention context, FIP Personnel may engage with potential field contacts

for the limited purposes of determining whether the potential field contact is a U.S. person or possesses—

- (A) Intelligence or information concerning national or homeland security threats or vulnerabilities that is appropriate for Intelligence Community, departmental, or FSLTTP audiences, but would not otherwise be reported to those audiences; or
 - (B) Intelligence or information, or access to intelligence or information, that makes them a viable candidate for persistent contact with the Intelligence Community or an FSLTT law enforcement agency as an intelligence or law enforcement source.
- (ii) FIP Personnel are prohibited from using pre-interview engagements with potential field contacts to solicit intelligence or information for intelligence purposes other than to assess their viability as field contacts, and FIP Personnel are prohibited from using such engagements to solicit intelligence or information for use in intelligence reports under any circumstances.
- (iii) FIP Personnel must confirm that other relevant Intelligence Community and federal law enforcement partners are unwilling or unable to report such intelligence or information before pursuing a field interview outside the administrative detention context.

(b) Overtness and Voluntariness. Field interviews must be overt to the field contact, meaning that they are openly acknowledged by, or readily attributable to, the U.S. Government, or would be acknowledged in response to an express inquiry; and voluntary, meaning the intelligence or information is not obtained through coercion or intimidation.

- (i) FIP Personnel are prohibited from requiring a potential field contact to participate in a field interview; exercising, arranging, or facilitating any prejudicial or preferential treatment in exchange for participation; preventing the contact from terminating an interview at any time; or stating or implying anything to the contrary to the contact.
- (ii) FIP Personnel are prohibited from making any promise to the field contact in exchange for intelligence or information, including, but not limited to, financial remuneration, criminal charge consideration, change of immigration status or benefit to the field contact, or guarantee of any outcome.
- (iii) FIP Personnel are prohibited from changing, or attempting to change, the location at which field contacts in law enforcement or administrative detention are held (other than for the duration of the field interview).
- (iv) [Redacted.]

(c) Protections for U.S. Persons. Generally, FIP Personnel do not conduct field interviews of U.S. persons; however, they may conduct field interviews of U.S. persons not in administrative detention under the limited circumstances set forth in Section 4-201-01(b)(ii) above. FIP Personnel may not conduct field interviews of U.S. persons under any circumstances absent a reasonable belief that the field contact possesses significant foreign intelligence.

(i) Consistent with applicable law, executive order, and I&A's Intelligence Oversight Guidelines, "foreign intelligence" means information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, foreign persons, or international terrorists.

(ii) Generally, it is reasonable to expect that a field contact possesses significant foreign intelligence where a substantial amount of the information that I&A expects to receive from the contact is responsive to a valid, identified Intelligence Community (i.e., not just departmental) collection requirement with a foreign nexus or I&A expects to receive information highly responsive to a valid Intelligence Community collection requirement.

(iii) There is no minimal volume of foreign intelligence that must be provided by a field contact for it to be significant, but if the amount and importance of the expected foreign intelligence is trivial compared to the amount and importance of non-foreign intelligence expected from the contact or is incidental to it, that foreign intelligence generally will not be considered significant.

(d) Protections for Field Contacts in Law Enforcement Custody or Facing Criminal Charges. I&A generally does not conduct field interviews of individuals in law enforcement custody (as distinguished from individuals in DHS administrative detention); however, FIP Personnel may do so under the limited circumstances set forth in Section 4-201-01(b)(ii) above, and I&A may interview individuals in administrative detention or otherwise who are facing criminal charges. Field interviews of individuals in law enforcement custody or who are facing criminal charges give rise to special legal, privacy, and civil liberties considerations for those field contacts. Accordingly, I&A provides the following additional protections for such individuals:

(i) Prior to conducting any field interview, FIP Personnel will take reasonable steps to determine whether potential field contacts not currently in law enforcement custody have been criminally charged or arraigned and, if so, whether their guilt with respect to such matters has been fully adjudicated (including sentencing). At a minimum, this requires a records check of the proposed interviewee in DHS systems that contain such information and are available to FIP Personnel.

(ii) In the event that FIP Personnel identify a potential field contact who is currently in law enforcement custody or who has been criminally charged or arraigned and whose

guilt has not yet been adjudicated, or, having been adjudicated as guilty, has not yet been sentenced, FIP Personnel may not conduct an interview with that person, or otherwise engage that individual for collection purposes, unless they have obtained the consent of the field contact following the field contact's consultation with counsel.

(A) Absent express waiver from the USIA after consultation with the DUS/C, the DUS/P, OGC/ILD and TOPO/PIOB, the potential field contact's consent must also be acknowledged in writing.

(B) FIP Personnel are prohibited from interviewing potential field contacts meeting the criteria set forth in Section 4-201-06(d) above if the field contact is not represented by counsel.

(iii) Any such interviews must be conducted pursuant to standard operating procedures issued by the DUS/C and DUS/P and coordinated with OGC/ILD, TOPO/PIOB, the DHS Privacy Office (PRIV), and the DHS Office for Civil Rights and Civil Liberties (CRCL). These procedures will reflect the requirements described in Section 4-201-06(d)(i)-(iii) above.

(e) Deconfliction and Coordination.

(i) Field interviews must be deconflicted at the local level in advance with other relevant Intelligence Community, departmental, and law enforcement partners.

(A) FIP Personnel must use classified and unclassified systems available to them to facilitate this deconfliction.

(B) In advance of a potential field interview, FIP Personnel may obtain information, including PII, necessary to conduct this deconfliction.

(ii) Where they identify intelligence, law enforcement, or other departmental equities in a potential field contact, FIP Personnel work with interested partners to ensure any questions or concerns they have regarding the field interview are addressed. This may include coordination with the Federal Bureau of Investigation's Joint Terrorism Task Forces.

(iii) Field interviews with contacts in law enforcement custody or referred to I&A from law enforcement agencies must be coordinated in advance with that agency.

(f) Location. FIP Personnel are permitted to conduct field interviews in neutral locations such as a government or commercially owned office or conference room. They are prohibited from conducting field interviews in non-neutral locations, including, but not limited to, any environment reasonably likely to distract or influence the contact or FIP Personnel in the

conduct of their interview (e.g., at a contact's home or anywhere unsafe), unless they receive permission to do so via an approved OPSPRO describing the environment.

(g) Required Disclosures.

(i) To help ensure that field interviews are overt and voluntary, and to comply with statutory requirements, FIP Personnel must explain to a field contact and request acknowledgment that—

(A) The interviewer is an employee of the U.S. Department of Homeland Security;

(B) The contact's participation is voluntary;

(C) The interview may be terminated by either party at any time;

(D) The interviewer will not exercise any preferential or prejudicial treatment in exchange for the contact's cooperation;

(E) For field contacts in administrative detention, that the interview is not being conducted in connection with an immigration proceeding, but intelligence or information provided through the interview may be used or shared for purposes of making an immigration determination to the extent permitted by, and consistent with, applicable law and regulation;

(F) For field contacts in law enforcement custody or who have been criminally charged or arraigned and whose guilt has not yet been adjudicated, or, having been adjudicated as guilty, have not yet been sentenced, that they have the right to have counsel present at the interview; that they may consult with their attorney at any point during the interview; and that the interview is not being conducted in connection with their criminal case, but that intelligence or information provided through the interview may be used or shared for that purpose to the extent permitted by, and consistent with, applicable law and regulation.

(G) Either—

(I) That the contact has not, to the best of the contact's knowledge, been criminally charged or arraigned by a federal, state, or local law enforcement agency with respect to any criminal matters that have not already been adjudicated; or

(II) If the contact is in law enforcement custody or is reasonably believed to have been criminally charged or arraigned by a federal, state, or local law enforcement agency with respect to criminal matters that have not been adjudicated, that the contact consents to the interview following consultation with their counsel;

(H) The contact has no right to review, edit, or control I&A's use of any intelligence or information collected and products derived from the interview except to the extent provided by the Privacy Act of 1974 and the Freedom of Information Act; and

(I) Any other disclosures required by the standard operating procedures to be issued jointly by the DUS/C and DUS/P.

(ii) FIP Personnel must ask potential field contacts to sign a pre-interview form (whether physical or digital) that acknowledges receipt and understanding of the disclosures required by Section 4-201-06(g)(i) above. Should a prospective contact indicate that they are unable or unwilling to sign the form, or if circumstances surrounding the interview make it impracticable for a form to be used (e.g., the interview occurs in a location where the form is unavailable), the interview may proceed so long as the contact otherwise acknowledges receipt and understanding of the disclosures required by Section 4-201-06(g)(i) above; however, under those circumstances, both the interviewer and at least one witness must certify in writing that the potential contact acknowledges and understands the provisions. This record is appended to, or maintained contemporaneous with, the contact memorandum for the interview.

(h) Prohibition on Firearms. To ensure that field interviews are free from any perception of coercion, threats, or intimidation, FIP Personnel may not carry firearms on their person when engaging in field interviews.

4-201-07. Contact Memorandum. Following each liaison exchange, field interview, or preliminary engagement with a potential field contact, FIP Personnel must complete a contact memorandum to ensure an accurate and comprehensive understanding of the exchange, interview, or preliminary engagement for future use and oversight.

(a) Contents. All contact memoranda must characterize the circumstances surrounding a liaison exchange, field interview, or preliminary exchange with a potential field contact, including information about the liaison, field, or potential field contact, and identify any operational, counterintelligence, or other concerns with the exchange, interview, or preliminary engagement. For auditing purposes, contact memoranda must also include the name(s) of the interviewer(s), the time and place of the exchange, interview, or preliminary engagement, and any raw intelligence report arising from the contact.

(b) Additional Contents for Field Interviews. In addition to the contextual information described in Section 4-201-07(a) above, contact memoranda for field interviews must describe—

(i) The provision (including the quantity and value) of any items of monetary value to field contacts, including *de minimis* items such as food, water, or tobacco items;

(ii) Consistent with Section 4-201-06(g)(i)(G) above, the field contact's response as to whether, to the best of their knowledge, the contact has been criminally charged or arraigned by a federal, state, or local law enforcement agency and, if so, whether their guilt with respect to such criminal matters has already been adjudicated or they consent to the interview following consultation with counsel; and

(iii) For field interviews of U.S. persons, and consistent with Section 4-201-06(c) above, a description of the foreign intelligence (along with any non-foreign intelligence) obtained from the U.S. person(s).

(c) Timing. Contact memoranda must be completed not more than five days after the liaison exchange, field interview, or preliminary engagement with a potential field contact. This deadline may be extended by the supervisor of the I&A personnel conducting the exchange, interview, or preliminary exchange provided the extension is memorialized and the supervisor establishes a new deadline for completion of the contact memorandum in writing, which may not exceed 30 days after the exchange, interview, or preliminary engagement.

4-201-08. Reporting. FIP Personnel report intelligence and information obtained through liaison exchanges or field interviews in Intelligence Information Reports (IIRs) (for intelligence and information responsive to Intelligence Community collection requirements), Field Intelligence Reports (FIRs) (for intelligence and information responsive only to departmental collection requirements), or Homeland Targeting Lead Cables (for targeting leads that do not meet the criteria for reporting IIRs or FIRs). FIP Personnel may also provide operational referrals to law enforcement or Intelligence Community partners.

4-201-09. Temporary Waivers. The DUS/C and DUS/P, to the extent permissible under law, executive order and presidential memorandum, regulation, international agreement and obligation, and national and departmental policy (including I&A's Intelligence Oversight Guidelines), may temporarily waive any provision of this policy guidance where required to respond to exigent threats.

(a) Criteria.

(i) Exigent threats are specific, credible, threats arising in the prior 90 days, or reasonably likely to arise in the succeeding 90 days, to the United States, its people, or vital national interests (either domestically or abroad) where the collection of intelligence or information by I&A personnel is reasonably likely to further the efforts of the United States to counter such threats.

(ii) Any temporary waiver, in the assessment of the DUS/C and DUS/P, must be necessary to enable the collection of such intelligence or information (i.e., the collection could not occur otherwise consistent with the provisions of this policy guidance).

(b) Process.

(i) Any FIP Personnel may request a temporary waiver from the DUS/C and DUS/P through their supervisory chain of command to the Director of FID, who will refer the request to the DUS/C and DUS/P for decision. Non-FIP Personnel may submit a request for a temporary waiver through their supervisory chain of command to their cognizant Deputy Under Secretary or, for personnel in the I&A front office, the Chief of Staff, prior to referral to the DUS/C and DUS/P for decision. Alternatively, the DUS/C or DUS/P may decide to pursue a temporary waiver on their own initiative.

(ii) The DUS/C and DUS/P will coordinate any temporary waiver with the AGC/Intel to ensure the legal sufficiency of any temporary waiver and with the D/TOPO to ensure the protection of privacy, civil rights, and civil liberties in any temporary waiver.

(A) The D/TOPO will consult with PRIV and CRCL on any novel or complex matters pertaining to privacy, civil rights, or civil liberties arising from a proposed temporary waiver.

(B) Any disagreements between the DUS/C or DUS/P and the AGC/Intel or D/TOPO concerning a proposed temporary waiver will be elevated immediately for resolution.

(iii) A temporary waiver may only be issued where both the DUS/C and DUS/P agree to do so. Any disagreement between the DUS/C and DUS/P will be elevated immediately for resolution by the USIA or Principal Deputy Under Secretary for Intelligence and Analysis.

(iv) A temporary waiver may not last beyond the duration of the exigent threat or 90 days, whichever occurs first. If an exigent threat extends beyond 90 days, the DUS/C and DUS/P must request approval of any further extension by the USIA in consultation with the AGC/Intel, D/TOPO, and, for waivers of provisions that result in material infringements of individuals' privacy, civil rights, or civil liberties, the DHS Chief Privacy Officer and DHS Officer for Civil Rights and Civil Liberties.

(v) The DUS/C will memorialize any temporary waiver, including the exigent threat giving rise to the waiver and why the waiver is necessary to collect intelligence or information reasonably likely to further the efforts of the United States to counter the threat, not later than 30 days from the date of the issuance of the temporary waiver. The DUS/C will provide copies of this memorialization to the DUS/P, AGC/Intel, and D/TOPO.

4-202: Engaging Partners in the Field

Office of Intelligence and Analysis (I&A) senior leadership identified a need to reinforce the role of the Field Intelligence Directorate (FID) and its regional directors as I&A’s primary representatives to federal, state, local, tribal, territorial, and private sector (FSLTTP) partners in the field. This policy guidance addresses the responsibilities of I&A personnel assigned, detailed, deployed, or conducting official travel to one or more of FID’s ten regions. It provides amplifying procedures related to the role of FID and its regional directors based on Intelligence Community best practices. It also sets forth notification and coordination requirements to foster a unified, regionally focused approach to engaging homeland security partners and supporting departmental priorities nationwide.

(a) Application. All I&A personnel will adhere to the procedures below for engaging partners in the field. This policy guidance applies specifically to I&A personnel not assigned to FID and does not include details or assignments to other departments’ or agencies’ headquarters offices or routine engagements occurring in the National Capitol Region with federal partners.

(b) Procedures.

(i) Before traveling to a FID region for operational support activities or engagements, I&A personnel will obtain written concurrence, via memorandum, from the regional director of the respective region prior to travel to the region.

(A) The memorandum must detail—

- (I) The purpose of the visit;
- (II) Its timeframe;
- (III) Expected participants; and
- (IV) Intended outcome(s).

(B) Directorate, center, and division directors also are expected to make every effort to provide at least two weeks’ notice of intended travel to the Director of FID (D/FID) and the respective regional director.

(C) If and when the relevant regional director agrees to the travel, I&A personnel seeking to travel to the region must provide the signed memorandum to the Deputy Under Secretary for Partnerships before making travel arrangements.

(ii) I&A personnel engaging virtually with FSLTTP partners outside the National Capitol Region must notify the regional director of the respective FID region prior to the virtual activity unless the outreach is at a national level, in which case they will notify the D/FID of the virtual engagement.

(iii) The Principal Deputy Under Secretary for Intelligence and Analysis will approve permanent or long-term placement of I&A personnel in the field. Mission managers and division directors are expected to coordinate with the D/FID and respective regional directors on the proposed placement of personnel before seeking approval. This does not include personnel assigned to FID.

4-203: Use of Government Vehicles by Field Personnel

This section is a placeholder. The policy will be included in a future version of the Policy Manual.

PART FIVE: MANAGEMENT

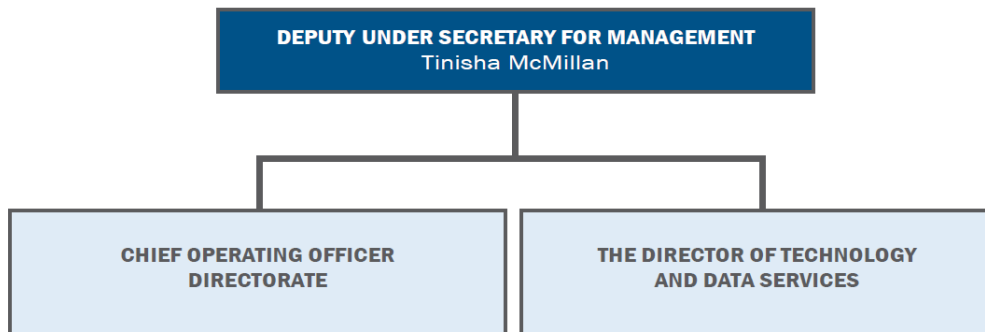
5-101: Organization of the Office of Management

The Office of Management is charged with supporting the successful execution of the intelligence mission and activities of the Office of Intelligence and Analysis (I&A). This includes overseeing I&A’s facilities and security apparatus; planning, resourcing, and budgeting capabilities; performance measures; human resource functions; training and talent management; and technology and data services.

The Office consists of two directorates: the Chief Operating Officer Directorate and the Directorate of Technology and Data Services.

(a) The Directorate of Chief Operating Officer. The Directorate of the Chief Operating Officer (COO) ensures the administrative support of I&A’s operations. It comprises five elements: the Mission Assurance Division, Financial Resources Management Division, Program and Performance Evaluation Division, Intelligence Training Academy, and Workforce Management and Engagement Division.

(b) The Directorate of Technology and Data Services. The Directorate of Technology and Data Services (TDS) provides DHS with intelligence mission systems that enable secure information sharing, collaboration, and analysis with federal, state, local, tribal, territorial, and private sector partners to protect the homeland by facilitating access and usability of data and analytics across the DHS Intelligence Enterprise, analytic centers, and relevant national security partners by providing enriched data at the speed of mission and capturing enterprise-wide relationships between mission and technology, TDS has six divisions: the Business Management Division, Cyber Security Division, Data Analytics and Information Sharing Division, Enterprise Architecture Division, Mission Solutions Division, and Information Technology Operations Division.



5-102: Employee Recruitment, Selection, Conversion, and Promotion

This section is a placeholder. The policy will be included in a future version of the Policy Manual.

5-103: Temporary Assignments, Extended Leave, and Management of Detailees

This policy guidance establishes the parameters and procedures for temporary assignments, the management of detailees, and the management of positions when Office of Intelligence and Analysis (I&A) personnel go on temporary assignments, including, but not limited to, detail assignments and extended leave. This guidance applies to all I&A personnel.

(a) Temporary Assignments. Temporary assignments promote the development of I&A personnel through exposure to other agencies and through the acquisition of competencies that would be difficult for the employee to obtain in their regular position or organization. Temporary assignments may include Department of Homeland Security (DHS) rotational programs, Intelligence Community Joint Duty Assignments, positions I&A contributes to the National Counterterrorism Center and other Intelligence Community organizations, and other *ad hoc* rotational opportunities.

(i) All temporary assignment requests are managed by the Workforce Management and Engagement Division within the Office of Management (WM&E) and require review and approval by the Under Secretary for Intelligence and Analysis.

(ii) I&A personnel are responsible for identifying temporary assignments and speaking about and assessing those opportunities with their immediate supervisors.

(iii) I&A personnel approved for temporary assignments maintain their official positions in their home offices (as shown on their most recent Form SF-50) as well as their promotion or step increase eligibility. Upon completion of their temporary assignment and return to their home office, employees may request reassignment or be reassigned based on the needs of I&A.

(A) Established and administered by Office of the Director of National Intelligence, the Intelligence Community Joint Duty Program, as described in Intelligence Community Directive (ICD) 660, *Intelligence Community Civilian Joint Duty Program* (Feb. 11, 2013), provides for—

(I) The detail of Intelligence Community civilian personnel to a position in another Intelligence Community element or other relevant organization that provides an Intelligence Community civilian joint duty qualifying experience; or

(II) The assignment of Intelligence Community civilian personnel to an approved internal position at the individual's employing element that provides an Intelligence Community civilian joint duty qualifying experience.

The purpose of the Joint Duty Program is to foster a community perspective and culture by providing Intelligence Community civilian joint duty qualifying experience(s) to Intelligence Community civilian personnel during their careers.

(B) Per ICD 660, an Intelligence Community civilian joint duty qualifying experience—

[P]rovides substantive professional, technical, or leadership experience that includes policy, program, managerial, analytical, or operational responsibility for intelligence resources, programs, policies, analysis, or operations in conjunction with one or more other Intelligence Community elements, or relevant organizations external to the Intelligence Community. A joint duty qualifying experience provides a wider understanding of the missions and functions of the Intelligence Community, or the Intelligence Community's relationships with relevant organizations outside the Intelligence Community; develops a broader knowledge of the operations and management of the Intelligence Community; and helps to build collaborative networks.⁸

(C) All Intelligence Community civilian intelligence professionals at the GS-11 or equivalent grade up to senior levels are eligible to participate in the Joint Duty Program. All candidates must receive supervisor and leadership endorsement to maintain their eligibility for the Joint Duty Program. ICD 660 requires at least one joint duty rotation (though this requirement may be waived at the discretion of the Director of National Intelligence) for promotion to senior-level officer positions in the Intelligence Community. Rotations generally last for two years, with a participant option to extend for another year. Extensions must be approved by the gaining agency, home agency, and the employee.

(b) Management of Detailees.

(i) Placing a detailed employee at a partner agency requires that a Memorandum of Agreement (MOA) be signed by the employing agency, the gaining agency, and the employee being detailed. WM&E coordinates with external components and agencies to process all MOAs and obtains the approval of necessary I&A signatories. WM&E will solicit MOA language from the responsible office regarding specific duties of incoming and outgoing detailees.

(ii) Detailees are subject to the operational control and direction of the gaining agency unless otherwise specified and agreed to by both parties to the governing MOA (e.g., in the case of assignees and liaison officers, which continue to fulfill certain responsibilities for their employing agency—see Section 4-102 for more information on I&A's Liaison Officer Program).

(iii) A detailee is an employee of one federal agency or department (employing agency) who, through formal agreement with another federal agency or department (gaining agency), is temporarily placed with the gaining agency to perform duties for the gaining

⁸ ICD 660 § D.1.

agency and under the gaining agency's operational (but not administrative) control for a defined period of time.

(iv) Detailed employees are assigned to facilitate collaboration between agencies, represent the perspective of those agencies, and act as a general point of contact for conducting business with agency partners.

(v) Placing a detailed employee at a partner agency requires that an MOA be signed by the employing agency, the gaining agency, and the employee being detailed. WM&E's Human Capital Branch coordinates with external components and agencies to process all MOAs and obtains the approval of necessary I&A signatories. WM&E's Human Capital Branch will solicit MOA language from the responsible office regarding specific duties of incoming and outgoing detailees.

(vi) Details may be either reimbursable or non-reimbursable, as agreed to by the gaining and employing agencies in the governing MOA.

(vii) Detailees are subject to the operational control and direction of the gaining agency, unless otherwise specified and agreed to by both parties to the governing MOA (e.g., in the case of assignees and liaison officers, who continue to fulfill certain responsibilities for their employing agency).

(viii) A detailed employee's permanent position of record remains with the employing agency, and the employee remains on the permanent roster of that employing agency during the detail assignment unless other arrangements are agreed to by the employing and gaining agencies in the governing MOA.

(ix) Incoming detailees may supervise I&A employees only if a supervisory role is delineated and agreed to by both parties in the governing MOA.

(x) If an outgoing detail cannot be filled from the responsible office's existing resources, a request may be forwarded to WM&E's Human Capital Branch for an I&A-wide solicitation; however, responsibility for the outgoing detail billet remains with the responsible office.

(xi) I&A detail assignments to or from state and local governments, institutions of higher education, Indian tribal governments, and other eligible organizations are to be made pursuant to the Intergovernmental Personnel Act of 1970 (IPA). Such details are intended to facilitate cooperation between the federal government and the non-federal entity through the temporary assignment of skilled personnel. IPA details allow civilian employees of federal agencies to serve with eligible non-federal organizations for a limited period without loss of employee rights and benefits. Similarly, the IPA enables employees of state and local governments, Indian tribal governments, institutions of higher education, and other eligible organizations to serve in federal agencies for similar

periods. IPA details are processed in accordance with applicable DHS and I&A policies and guidance.

(c) Backfilling Positions Encumbered by Personnel on Temporary Assignments and Extended Leave. I&A encourages employees to broaden and develop skills through temporary assignments within I&A, DHS, and the Intelligence Community. While employees are away from their position of record, I&A also must sustain the role and functions of the positions they encumber, and within the authorized personnel limit for each subdivision or unit.

I&A does not permit permanent hires for positions that are only temporarily vacant; to do so would result in uncontrolled growth and displace persons on detail from their position of record. While I&A aims to provide new experiences for persons returning from a detail, all persons encumber their billet/position of record for the duration of their detail and until such time as they are permanently reassigned to another position.

Managers are encouraged to consult early with WM&E on strategies to backfill positions while enabling employees to take temporary assignments. The below options are available when an I&A employee goes on a temporary assignment:

- (i) Temporarily reassign a current I&A employee of equal grade to the position (through a management-directed reassignment or internal vacancy announcement);
- (ii) Temporarily promote a lower-graded employee into the position⁹;
- (iii) Fill the position through joint duty assignment (detail); or
- (iv) Leave the position unfilled.

⁹ The Director of WM&E is the point of contact for procedures governing the temporary promotion process. Employees accepting a temporary promotion must sign a statement of understanding acknowledging the conditions of the temporary promotion.

5-104: Leave, Premium Pay, Breaks, Alternative Work Schedules, Telework, and DHS Wellness Program

This policy guidance establishes the guidelines and procedures for leave, premium pay, breaks, alternative work schedules (AWS), and the implementation of the Department of Homeland Security (DHS) Telework and Wellness Programs within the Office of Intelligence and Analysis (I&A).

5-104-01. Leave, Premium Pay, Breaks, Alternative Work Schedules.

The following guidance establishes I&A policy for requesting and granting leave and premium pay, breaks during the workday, and AWS. It applies to all I&A employees except for DHS presidential appointees and employees who are identified as essential personnel during emergencies, perform shift work, or receive night differential. These exempt employees follow the guidance set forth by their respective offices.

The following guidance also applies to detailees supporting I&A and I&A employees detailed outside I&A unless prohibited by the personnel agreement governing the detail. It does not apply to contractors.

(a) Overview. The U.S. Government offers a wide range of leave options and workplace flexibilities to assist an employee who needs to be away from the workplace. These flexibilities include annual leave, sick leave, advanced annual leave or advanced sick leave, leave under the Family and Medical Leave Act of 1993 (FMLA), donated leave under the voluntary leave transfer program, leave without pay, alternative work schedules, credit hours under flexible work schedules, compensatory time off, and telework. Providing workplace flexibilities helps I&A achieve its goals of recruiting and retaining talent, increasing employee engagement, boosting employee morale, and fostering a diverse and inclusive workforce.

(b) Leave Requests.

(i) An employee may use annual leave for vacations, rest and relaxation, and personal business or emergencies. An employee has a right to take annual leave, subject to the right of the supervisor to schedule the time at which annual leave may be taken.

(ii) Employees and their supervisors are mutually responsible for planning and scheduling the use of employees' annual leave throughout the leave year. Employees should request annual leave in a timely manner, and supervisors should provide timely responses to employees' requests.

(iii) When an employee makes a timely request for leave, the supervisor must either approve the request and schedule the leave at the time requested by the employee or, if scheduling leave is not possible because of mission needs, the supervisor must coordinate

with the employee to schedule it at some other time. Employees may appeal leave decisions to the second-line supervisor, whose decision is final.

(iv) Acting supervisors are authorized to approve leave that is scheduled during the period for which they are expected to be in an acting supervisor capacity. If the acting supervisor does not have sufficient permissions in WebTA (or any successor system), the acting supervisor makes the decision on the leave request, emails approval to the second-line supervisor, who will approve the leave request in WebTA.

(v) If the employee's supervisor is absent, and no acting supervisor has been designated, the employee contacts the second-line supervisor in the supervisory chain. Unless designated as an acting supervisor, co-workers are not authorized to approve leave.

(vi) Employees ensure that direct contact is made with the supervisor or acting supervisor to receive confirmation that the employee's requested leave is approved.

(vii) The advance notice requirement does not apply to emergency situations or for unscheduled sick leave requests. Employees requesting emergency leave or unscheduled sick leave contact their supervisor within the first hour of their scheduled shift using a communication method prescribed by the supervisor. A leave request in an emergency situation does not automatically result in approval. If unanticipated emergency or sick leave is granted, once able, employees submit leave requests via WebTA and modify the timecards, as appropriate.

(viii) Supervisors may require a medical certificate or other administratively acceptable evidence for sick leave requests of longer than three consecutive workdays, or for a lesser period when determined necessary by the supervisor. I&A may consider an employee's self-certification as to the reason for their absence as administratively acceptable evidence regardless of the duration of the absence. An employee must provide administratively acceptable evidence or medical certification within 15 calendar days of I&A's request. If the employee is unable to provide evidence, despite the employee's diligent, good faith efforts, they must provide it within a reasonable period of time, but not later than 30 calendar days after I&A makes the request. If the employee fails to provide the required evidence within the specified time period, they are not entitled to sick leave.

(ix) If any employee is scheduled to be absent on the last day of a pay period, the employee must complete and validate their timecard in advance. If the employee is prevented from completing their timecard in advance (e.g., due to an emergency or unscheduled sick leave), the timekeeper and supervisor can create and certify an employee timecard.

(x) Supervisors may require advance notice from employees requesting annual leave for purposes of balancing workloads for the work unit (e.g., summertime and holidays to ensure appropriate staffing levels).

(xi) Supervisors may cancel approved annual leave due to mission requirements. I&A does not reimburse employees who have incurred personal expenses related to the annual leave.

(xii) Supervisors may place employees who fail to report to work (i.e., within one hour of regular start time) or who have not obtained approved leave on leave restrictions or absence without leave (AWOL) status (or both). Supervisors should contact DHS's Employee Relations Office within the Management Directorate's Office of the Chief Human Capital Office to consult on any restriction or AWOL actions before implementation.

(c) Premium Pay Requests.

(i) Premium pay (i.e., compensatory (comp time), credit hours, and overtime) is authorized when I&A mission needs require an employee to work longer than normal hours. A supervisor cannot require an employee to work more than their normal duty hours without offering the appropriate premium pay option. Premium pay is not used for rewarding performance.

(A) An employee must be assigned to a flexible work schedule (FWS) to receive credit hours.

(B) A full-time employee is limited to carrying over 24 credit hours from a biweekly pay period to a succeeding biweekly pay period.

(C) Senior Executive Service (SES) members may participate in FWS programs; however, they may not accumulate credit hours.

(ii) Premium pay is to be authorized in writing (e-mail), in advance, and by an employee's supervisor or designated acting supervisor. Overtime is approved at the Branch Chief-level or higher to ensure budgetary resources are available. Only comp time and credit hours can be approved by an acting supervisor as well as a Branch Chief.

(iii) Differentials (Night Differential and Sunday Differential) are only authorized for regularly scheduled work, meaning work that is scheduled in advance of the employee's administrative workweek. Employees on FWS who choose to work at night, on holidays, or on Sundays to meet the hourly requirement may not receive Sunday premium pay, holiday premium pay, or night differential pay.

(iv) Authorized premium pay is submitted by the employee in WebTA after receiving the advance written approval by their supervisor and the additional work hours are completed.

(d) Basic Work Schedules.

(i) The workday for employees on basic work schedules lasts eight (8) hours of work time or eight and a half (8.5) hours with 8 hours of work time and thirty (30) minutes for an unpaid break taken during the assigned work shift.

(ii) Employees may extend the unpaid break for up to 30 minutes by—

(A) Using annual leave, comp time, or award time; or

(B) Extending workday hours to ensure the paid 8-hour workday is completed in full (e.g., if the employee starts the workday at 8:00 a.m. and takes a 30-minute break, the end of the workday is 4:30 p.m.; if the employee takes a one-hour break and does not use leave, then the end of the workday becomes 5:00 p.m.).

(e) Alternative Work Schedules.

This sub-section of Section 5-104-01 is a placeholder. The policy will be included in a future version of the Policy Manual.

5-104-02. Telework.

Telework is a longstanding practice that can be an efficient and effective way of fulfilling departmental missions. This was especially true during prior phases of the COVID-19 pandemic, which required a broader approach to Telework as an important tool for safely and efficiently delivering mission-critical services. As the threat from COVID-19 becomes more akin to that of other common respiratory viruses, departments and agencies, including DHS, are working to increase their in-person presence, especially for those in support components (i.e., headquarters elements) who work in the National Capital Region. The DHS Telework Program balances these interests by providing a program that enhances employee and organizational performance, recruitment, retention, cost savings, and work-life balance.

As a support component participating in the DHS Telework Program, I&A supports and encourages telework flexibilities for eligible employees consistent with the need to achieve its mission goals and objectives. The provisions below implement the DHS Telework Program for I&A, setting guidelines and expectations for telework that reflect I&A's special organizational needs for in-person collaboration and engagement as well as access to classified information for most positions.

(a) General Framework for Implementation of the DHS Telework Program.

(i) Under federal law, agency employees are generally ineligible for telework where their official duties require them daily (i.e., every workday) to (1) directly handle secure materials that are inappropriate for telework or (2) engage in onsite activities that cannot be handled remotely or at an alternate worksite (i.e., an approved location where official duties are performed away from the regular worksite through telework or remote work such as an employee's residence, a telework center, a satellite office, or other approved location). I&A ensures its employees can conduct necessary activities by designating positions within the organization that satisfy these statutory requirements as telework eligible positions.

(ii) I&A's implementation of the DHS Telework Program includes both routine telework and situational telework. Routine telework is telework that occurs on a regular, recurring basis for one or more days per pay period. Situational telework is telework that occurs on an occasional, episodic, or short-term basis. Situational telework includes, but is not limited to telework that occurs on a temporary basis while an employee is recovering from an injury or illness, as a result of a special work assignment, or when the regular worksite is closed due to an emergency situation.

(A) The availability of either or both types of telework to specific I&A employees depends on (1) the nature and duties of the employee's position as determined by their cognizant Senior Telework Official (i.e., the head of their respective subcomponent (Analysis, Partnerships, Management, Collection, the Front Office, the Transparency and Oversight Program Office, and the Intelligence Enterprise Program Office) and (2) satisfaction of the eligibility criteria for general participation in the program set forth in Section 5-105-02(c) below.

(B) Supervisors are responsible for ensuring sufficient coverage at the regular worksite(s) for their work units at all times.

(iii) I&A's implementation of the DHS Telework Program features "core days" (Tuesdays and Thursdays) where routine telework is not permitted during the "core hours" of 10:00 a.m. to 2:00 p.m.

(A) Core days are an important mechanism to ensure that I&A employees build professional relationships, work together towards common goals, and help to develop a common culture for I&A.

(B) The requirement to work from the employee's regular worksite during core hours on core days only applies to employees whose official worksite is the St. Elizabeths Campus or Nebraska Avenue Complex and whose assigned work hours encompass core days and core hours. These employees are referred to throughout this policy guidance as "covered employees."

(iv) Supervisors determine specific telework schedules for their subordinate employees in telework eligible positions who seek to engage in telework. Telework schedules must be consistent with this policy guidance and memorialized via telework agreements approved by supervisors to ensure the terms and conditions of the telework agreement comply with this policy guidance.

(v) I&A employees engaging in telework are subject to the same performance requirements and standards of conduct that apply to employees when not teleworking.

(A) Employees engaging in telework have the same opportunities and requirements for purposes of all work obligations, performance management, training opportunities, awards and recognition, assignments and reassignments, promotions, reductions in grade, and retention.

(B) Employees continue to be bound by DHS and I&A policies, procedures, and standards while teleworking at their alternate worksite or using government furnished equipment (GFE). Employees must follow appropriate administrative, technical, and physical safeguards at all times.

(C) Supervisors must communicate their expectations to employees for employee performance and accountability, including their expectations regarding office coverage, communication, and availability.

(vi) Authorization to telework is contingent on the ability of the I&A employee to work at their alternate worksite.

(A) If the employee is unable to work at their alternate worksite (e.g., due to physical damage or loss of electricity or internet support to the alternate worksite), they are required to notify their supervisor immediately and prepare to work from their regular worksite as soon as possible or to take leave.

(B) At all times teleworking employees are required to maintain a safe work environment when their alternate worksite is their residence.

(vii) Telework is a privilege, not a right. An employee's participation in the DHS Telework Program may be terminated at any time consistent with the procedures set forth in Section 5-104-02(f)(iv) below.

(b) Telework Position Determinations.

(i) Senior Telework Officials determine whether positions within their respective offices are Telework Eligible and, if so, whether these positions are eligible for situational telework, routine telework, or both.

- (A) Routine telework is generally appropriate for I&A employees in positions whose assigned duties are suitable for recurring Telework at an alternate worksite for one or more days each pay period.
- (B) Situational Telework is generally appropriate for I&A employees whose assigned duties are suitable for work at an alternate worksite on an episodic basis, including, but not limited to, when that employee is recovering from an injury or illness (but is still able to work) or working on a special work assignment of short duration, where their regular worksite is closed due to weather or other emergency situations, or to ensure the continuity of government operations during a continuity of operations event such as a pandemic health crisis.
- (ii) Senior Telework Officials make these determinations based on current mission requirements, required access to classified information, operational needs, positions responsibilities, equipment access, staffing needs, and whether employees can accomplish their regular, onsite essential mission functions offsite, as well.
- (iii) Senior Telework Officials consult with the Principal Deputy Under Secretary for Intelligence and Analysis (PDUSIA), the Deputy Under Secretary for Management (DUS/M) and their managers and supervisors when making these determinations.
- (iv) For each position determined by a Senior Telework Official to be eligible for routine telework, the cognizant Senior Telework Official, in consultation with the PDUSIA, DUS/M, and their managers and supervisors, also establishes a maximum number of days that employees occupying those positions may telework.
- (A) Senior Telework Officials and employees in management, supervisory, or other leadership positions (e.g., division directors, branch chiefs, section chiefs, or team leads) may be permitted to engage in routine telework for one day per pay period.
- (I) By default, all positions at the GS-14 level or above are presumed to be management, supervisory, or other leadership positions for the purposes of Section 5-104-02(b)(iv) above. Nevertheless, Senior Telework Officials may waive the application of this presumption on a position-by-position basis.
- (II) Senior Telework Officials may also identify positions at lower grades as management, supervisory, or other leadership positions for purposes of Section 5-104-02(b)(iv) above according to their discretion.
- (B) For positions that are not management, supervisory, or leadership:
- (I) Generally, the maximum amount of routine telework available is up to two days per pay period.

(II) For positions that, as determined by the Senior Telework Official, need less frequent in-person collaboration and only limited access to classified information, the maximum amount of routine telework available is up to four days per pay period.

(C) I&A employees seeking permission to engage in routine telework above the maximum amounts for their position as determined by their cognizant Senior Telework Official may pursue a waiver consistent with Section 5-104-02(g) below.

(D) Regardless of the position they occupy, no I&A employee may telework for more than eight days per pay period consistent with legal restrictions on the use of telework.

(v) Senior Telework Officials notify the Director of WM&E (D/WM&E) and their employees of their telework position determinations not later than 30 days after the commencement of employment.

(c) General Requirements for Telework Program Participation.

(i) Within I&A, only telework eligible employees may participate in the DHS Telework Program.

(A) To be telework eligible, I&A employees must—

(I) Occupy a telework eligible position;

(II) Be on a supervisor-approved performance work plan;

(III) Have a performance rating of “achieved expectations” or higher on their last performance rating of record and not currently be on a performance improvement plan;

(IV) Not currently be enrolled in a formal training program that requires the employee to report to a designated training site during official duty hours;

(V) Complete the telework training course; and

(VI) Possess GFE configured with a DHS-certified encryption software package and proper security controls for telework.

(B) If an employee does not have an approved performance work plan or current performance rating on file, the employer’s supervisor determines if the employee’s current performance is at an acceptable level to permit telework program participation.

(ii) I&A employees on a compressed work schedule are eligible for situational telework, but not routine telework.

(iii) For routine telework, the I&A employee's approved alternate worksite must be inside the locality pay area of their regular worksite.¹⁰ For situational telework, the I&A employee's approved alternate worksite can be inside or outside the locality pay area of their regular worksite.

(iv) Covered employees may not engage in routine telework on core days (Tuesdays and Thursdays) and are expected to be at their regular worksite during core hours (10:00 a.m.-2:00 p.m.) unless on authorized travel, on approved leave, or otherwise authorized to be absent from work.

(v) Under no circumstances may an employee engage in more than eight days total of telework (whether routine telework, situational telework, or both) in a single pay period.

(vi) Telework hours are recorded under the appropriate telework code corresponding to the type of telework performed. Employees requesting overtime or comp time must obtain their supervisor's approval before commencing such work.

(vii) Telework ready employees (i.e., telework eligible employees with signed telework agreements) authorized to engage in situational telework or routine telework must telework on any workday when I&A is closed for any reason other than an official holiday. This includes working their scheduled tour of duty during partial workdays (delayed openings or early release days). In this situation, any telework is recorded under the telework code, not as overtime or comp time.

(viii) Employees engaging in any telework (whether situational or routine) must check in with their supervisor at least once during the workday.

(ix) The government is not responsible for operating costs associated with a telework ready employee using their residence as an alternate worksite (e.g., home maintenance, insurance, or utilities).

(x) Telework is not a substitute for dependent care (for children or for other family members). Employees engaging in telework must make other arrangements for family member care. An employee's supervisor may waive this requirement where there are extenuating circumstances.

(xi) Employees teleworking from non-secure alternate worksites (e.g., their residence) may only perform unclassified duties and responsibilities that can be completed via unclassified e-mail, telephone, fax, or other unclassified electronic means.

¹⁰ "Locality pay area" is a term of art that refers to (1) a main metropolitan area defined by the Office of Management and Budget and forming the basic locality pay area and, where criteria recommended by the Federal Salary Council and approved by the President's Pay Agent are met, and (2) areas of application. Areas of application are locations that are adjacent to the basic locality pay area and meet approved criteria for inclusion in the locality pay area.

(d) Process to Become Telework Ready.

(i) To become telework ready, telework eligible employees must propose a telework schedule—for routine or situational telework—for review by their supervisor for consistency with the requirements of this policy guidance.

(A) Employees are encouraged to verify position and employee eligibility and telework readiness and submit proposed telework agreements during their first week of employment with I&A.

(B) Telework eligible employees submit telework agreements for review by their supervisors using the digital form prescribed by the Office of the Chief Human Capital Officer.

(C) Supervisors must respond to a proposed telework schedule within 20 days of receipt of submission of the proposal.

(D) Supervisors must disapprove any proposed telework schedule that does not meet the requirements of this policy guidance, including, but not limited to the requirements for routine telework concerning core days and core hours for covered employees and the maximum number of Telework days permitted for the employee's position.

(E) Supervisors, in their discretion, may disapprove any proposed schedule that would conflict with the operational or staffing needs of the employee's work unit.

(ii) An employee whose proposed telework schedule is disapproved by their supervisor may appeal the supervisor's decision to their second-line supervisor. Decisions by the second-line supervisor are final.

(iii) Employees must have a completed, signed, and approved telework agreement in place before performing any telework, including situational telework.

(e) Engaging in Telework.

(i) When telework ready employees engage in routine telework, they generally do so consistent with their telework schedules.

(A) Employees may be recalled to work at their regular worksites on days they are scheduled to work at their alternate worksite due to emerging operational or staffing needs.

(I) Supervisors will notify these employees as soon as possible—preferably no later than the prior business day—if any unforeseen circumstances arise requiring the employee to report in-person to the regular worksite.

(II) Employees recalled to their regular worksites on a previously scheduled routine telework day may request that their routine telework day be rescheduled within the same pay period.

(B) I&A employees may, with the approval of their supervisors, reschedule a routine telework day to another workday within the same pay period provided such requests are episodic or on a short term basis.

(C) Supervisors may grant such rescheduling requests, and they will grant such requests where the employee was recalled to work, under the following conditions:

(I) There is no in-person reporting requirement on the rescheduled routine telework day;

(II) Rescheduling the routine telework day would not cause the employee to exceed the maximum number of routine telework days in the pay period; and

(III) The employee requests to reschedule their routine telework day not later than the workday before the originally scheduled routine telework day.

(D) A supervisor's decision regarding an employee's rescheduling request is final.

(ii) Telework ready employees may request situational telework on an ad hoc basis. Each instance of situational telework must be approved in advance by the employee's supervisor.

(A) Employees are encouraged to request situational telework as far in advance as possible.

(B) Supervisors may disapprove any requested situational telework that would conflict with the operational or staffing needs of the employee's work unit. The supervisor's decision to disapprove situational telework is final.

(f) Replacing or Terminating Telework Agreements.

(i) A replacement telework agreement is required within 30 days of any change in the employee's position or job description, including a temporary change in job description such as a detail within I&A. An I&A employee may replace their telework agreement at any time with the approval of their supervisor provided the terms and conditions of the new telework agreement satisfy the requirements for position and employee eligibility set forth in Section 5-104-02(b)-(c) above.

(ii) I&A employees may terminate existing telework agreements at any time. Supervisors may terminate existing telework agreements where the circumstances below exist provided that the employee's supervisor provides written notice of termination and its basis to the employee, the D/WM&E, and their cognizant Senior Telework Official.

- (A) The supervisor may terminate an existing telework agreement under the following circumstances:
 - (I) Where the I&A employee is no longer eligible to participate in the DHS Telework Program under the criteria set forth in Section 5-104-02(c) above;
 - (II) Where, according to the employee's supervisor or cognizant Senior Telework Official, the operational or staffing needs of the employee's work unit require the employee to work at their regular worksite without routine telework;
 - (III) The employee violates their telework agreement; or
 - (IV) Where it would be unlawful for the employee to telework.
- (B) Except where it would be unlawful for the employee to continue teleworking, termination does not go into effect until at least five working days after the supervisor provides written notice of the termination and its basis to the employee.
- (C) Employees are responsible for all relocation and related costs, such as the return of GFE, that the employee may incur from relocating back to their regular worksite.
- (iii) Except where it would be unlawful for an employee to continue teleworking, employees may appeal the termination of a telework agreement by submitting a request for review of the determination to their cognizant Senior Telework Official.
 - (A) The appeal should include (1) the terminated telework agreement; (2) a summary of the basis for the supervisor's decision; and (3) any information submitted by the employee in support of their appeal.
 - (B) The decision of the cognizant Senior Telework Official is final.
 - (C) The termination of an existing telework agreement is suspended pending any appeal to the cognizant Senior Telework Official. Where the cognizant Senior Telework Official determines that the termination of a telework agreement is appropriate, the termination does not go into effect until at least five working days after the Senior Telework Official provides written notice of the decision on the appeal to the employee.
- (iv) Employees subject to a telework agreement and their supervisors review the telework agreement at least once per year to determine whether the telework agreement requires replacement, modification, or termination.
- (g) Waivers.
 - (i) The Chief of Staff, following review by the Office of the General Counsel, may issue waivers to provisions of this policy guidance submitted by a Senior Telework Official consistent with applicable law and national and departmental policy.

(ii) The Chief of Staff memorializes any waiver for each employee subject to the waiver, with copies of the waiver provided to the Under Secretary for Intelligence and Analysis, PDUSIA, DUS/M, cognizable Senior Telework Official, the D/WM&E, the employee, the employee's supervisor, and the Office of the General Counsel. The D/WM&E maintains records of these waivers.

(iii) Allowing an I&A employee with a disability to telework may be a form of a reasonable accommodation. Requests to telework as a reasonable accommodation are processed in accordance with DHS's reasonable accommodation policies and procedures.

5-104-3. DHS Wellness Program.

This sub-section of Section 5-104 is a placeholder. The policy will be included in a future version of the Policy Manual.

5-105: Employee Recognition and Awards

This policy guidance establishes the parameters and procedures for the nomination, approval, and granting of employee awards and recognition at the Office of Intelligence and Analysis (I&A). It applies to all I&A employees, including detailees to I&A and liaison officers. It does not apply to performance awards granted to individuals in the Senior Executive Service, private citizens, or organizations, including contractors supporting I&, except honorary awards.

(a) Purpose of Rewards.

(i) Awards are an important tool for supervisors and managers to reward and retain employees in recognition of a meritorious personal effort, act, service, performance, or other superior achievement accomplished within or outside the employee’s assigned job responsibilities.

(ii) Supervisors and managers are held accountable for fair review and distribution of awards within their areas of control. Specifically, they—

(A) Review the accomplishments, achievements, contributions, and performance of all employees at least quarterly to determine award eligibility; and

(B) Recognize employees as quickly as possible when granting awards.

(iii) Anyone in I&A may make an award recommendation as an initiator. Outside the context of specific established awards criteria for the Department of Homeland Security (DHS) peer-to-peer awards, employees work through their supervisory chains to make such recommendations.

(b) Types of Awards.

(i) Monetary awards:

(A) A cash reward is a non-rating based monetary award that is in the form of a lump sum cash payment, which does not increase the employee’s rate of basic pay. It is based on tangible or intangible benefits to the government.

(B) A quality step increase is an expedited within-grade increase used to reward employees at all General Schedule grade levels who display high quality performance. It differs from a cash award in that it becomes a permanent part of an employee’s base pay.

(I) To be eligible for a quality step increase, an employee must be at step 9 or below of their grade level, have received an “Achieved Excellence” rating of record, have demonstrated sustained performance of a high quality that is

expected to continue over time, and must not have received a quality step increase within the preceding 52 consecutive calendar weeks.

(II) Supervisors and managers may not combine a cash or non-monetary award and a quality step increase for the same activity.

(III) The Workforce Management and Engagement Division within the Office of Management issues annual awards guidance outlining the number of permissible quality step increases that can be allocated per office for any given year based on an allocation from the DHS Management Directorate's Office of the Chief Human Capital Officer.

(ii) Non-Monetary Awards.

(A) Time-off awards are an alternate means of recognizing accomplishments of employees. I&A honors time-off awards given by other DHS components. Time-off awards—

(I) Cannot exceed 80 hours during a 12-month calendar period;

(II) Must be scheduled and used within one calendar year after the award is granted;

(III) May be carried across leave years if it is within the one-year calendar period;

(IV) Have no effect on annual leave carryover limitations;

(V) May not be used to circumvent sick leave balances or as a form of administrative leave;

(VI) Cannot be converted to cash under any circumstances;

(VII) Are not to be converted into any lump sum payment received by the employee upon separation from federal service;

(VIII) Are forfeited if an employee separates from DHS before using all time-off hours; and

(IX) Do not transfer to other agencies.

(B) Certificates or tokens may be given to employees in recognition of special acts, accomplishments, contributions, or other achievements contemplated in this policy guidance in addition to or in lieu of monetary or non-monetary awards for the same contribution.

(c) General Eligibility.

(i) All I&A employees are eligible for awards consistent with the criteria for those awards delineated in Section 5-105(b) above and using appropriate processes and procedures.

(ii) Monetary and non-monetary awards for employees detailed from I&A to positions outside I&A are determined by the hosting agency, component, or entity. Funding for reimbursable detailee award submissions is the responsibility of the hosting agency. The responsibility for determining whether to provide an award to an employee of another component, department or agency, or entity detailed to a position within I&A, as well as the responsibility for funding such an award, is established in the personnel agreement governing that individual's detail. I&A's preference is that awards for detailees to I&A positions be provided by I&A and, where the detail is reimbursable, funded by I&A.

(iii) Monetary or non-monetary awards for I&A employees assigned to a position that is embedded with, or located at, the facilities of another agency, component, or entity are determined by I&A consistent with I&A's award guidance set forth in section of the Policy Manual.

(iv) Monetary and non-monetary awards for I&A Liaison Officers are determined by I&A consistent with I&A's award guidance set forth in this Section of the Policy Manual. Because they officially remain in their old billet while in the Liaison Officer role, any awards for Liaison Officers should come out of the awards budget for their "home" division.

(v) There is a \$10,000 aggregate limit on the monetary award amount an individual can receive per year, even from a combination of multiple awards.

(d) Descriptions of Specific Awards.

(i) The on-the-spot award provides immediate recognition for non-recurring, high quality, short-term contributions involving a difficult or important issue, project, or assignment.

(A) On-the-spot awards consist of cash or time off.

(B) The total amount of an on-the-spot monetary award may not exceed \$1,000 or a 40-hour time-off period per individual for a specific contribution.

(C) The initiator—the person who suggests the granting of the award—recommends the amount of cash or time off.

(D) Approving officials preliminarily approve on-the-spot awards subject to final approval by the DHS Management Directorate's Office of the Chief Human Capital Officer.

- (E) Examples include, but are not limited to, displaying special initiative and skill in completing an assignment or project before its deadline; using initiative and creativity to improve a product, activity, program, or service; or completing additional work or a project assignment while maintaining the employee's own workload.
- (ii) The special act award is used to recognize exemplary performance more significant than that recognized by the on-the-spot award.
- (A) Special act awards may consist of monetary or time-off awards.
- (B) The total amount of an approving official may preliminarily approve shall not exceed \$10,000 or 80 hours time off.
- (C) For monetary special act awards, the employee is responsible for the taxes. A key difference between monetary on-the-spot awards and monetary special act awards is how the amount of the award is grossed-up to account for taxes. If an employee receives a \$500 on-the-spot award, the employee receives the full \$500 after taxes; approximately \$710 is taken from the division's awards budget. For monetary special act awards, the employee is responsible for the taxes.
- (D) Examples of contributions that would merit the granting of a special act award include, but are not limited to, the delivery of tangible benefits measurable in cost savings or more efficient operations; intangible benefits to the government; making scientific or technical advances; acting in an exemplary or courageous manner in an emergency situation related to official duties; publishing articles, presenting technical papers to professional organizations, or performing similar personal projects in a professional capacity that contribute significantly to the DHS mission; improving service to the public in a specific or measurable way; or notably improving DHS public relations.
- (iii) Listed below are recurring special act awards specifically tailored to recognize noteworthy individual or group contributions or to reinforce model behaviors for improving the I&A organization and building a coherent I&A culture. Each quarter, individual employees or employee teams, as appropriate, are nominated by each member of the I&A Senior Staff or by workforce initiators for each category below. The Under Secretary for Intelligence and Analysis (USIA), the Principal Deputy Under Secretary for Intelligence and Analysis (PDUSIA), and the Senior Staff will meet to discuss and make final selections.
- (A) Each member of a team awarded an Outstanding Team Citation will be given the choice between a \$500 on-the-spot award or a non-monetary recognition (8 hour time-off award), as well as a plaque commemorating the unit or group achievement. Eligibility is limited to employees, Joint Duty Program or other detailees to I&A from other government agencies, and I&A interns. Contractors are not eligible. Joint Duty

Program or other detailees may not be eligible for time-off awards depending on the terms of the memorandum of understanding for their assignment.

(B) Each recipient of an I&A Values Award receives a monetary award between \$3,000 and \$4,500 commensurate with the nature and magnitude of the employee's demonstrated act, behavior, or achievement.

(I) The "corporate give back" recognition celebrates I&A employee contributions to making I&A a better place and demonstrated commitment to something greater than themselves by strategically transforming workplace conditions to foster worker well-being and improve overall organizational resilience.

(II) The "innovation" recognition celebrates I&A employees who have pushed the organization to envision new possibilities for its internal and external workflows and impact.

(III) The "integrity" recognition celebrates I&A employees who demonstrated their commitment to protecting the rights of American citizens, as applied to the course of their duties.

(C) The Outstanding Supervisor Award is granted to supervisors who through their actions or achievements, or both, advance the mission, develop people, and foster a positive and inclusive team environment. The monetary award is between \$3,000 and \$4,500.

(D) The Employee of the Quarter award is granted to an employee who executes one or more exceptional actions or achieves something exceptional. The monetary award is \$6,000.

(E) The I&A Impact Awards are given to individuals who execute a particularly significant or impactful action or achieve something particularly exceptional over an extended period (at least six months). The monetary award is \$4,500, and a plaque is given commemorating their contribution. Like the I&A quarterly awards, the workforce and Senior Staff will be asked to nominate potential recipients each quarter. The USIA, PDUSIA, and Senior Staff will meet to discuss and make final selections prior to announcing recipients at an awards ceremony.

(e) Awards Ceremonies. Awards ceremonies are held to recognize quarterly award winners, length of service, professional achievements and service awards, and promotions.

5-106: Planning, Programming, Budgeting, and Evaluation Program

This section is a placeholder. The policy will be included in a future version of the Policy Manual.

5-107: Records and Information Management

Government organizations must manage their records effectively to ensure accuracy, accountability, and longevity. In addition to satisfying legal requirements, records management is necessary to ensure transparency in an agency's engagement with the public and in the broader democratic process. The Office of Intelligence and Analysis (I&A) consistently engages with a variety of federal and non-federal partners that would benefit from records management procedures that maximize and streamline access to valuable intelligence and information.

This policy guidance establishes standards for the effective and efficient management of I&A's electronic records throughout the Records and Information Management (RIM) lifecycle (creation, maintenance and use, and disposition) in line with relevant legal authorities and requirements.

(a) Overview.

(i) The Federal Records Act of 1950 requires all federal agencies to “make and preserve records containing adequate and proper documentation of the organization, functions, policies, decisions, procedures, and essential transactions of the agency and designed to furnish the information necessary to protect the legal and financial rights of the [U.S.] Government and of persons directly affected by the agency's activities.”¹¹ The law also requires agencies to “establish and maintain an active, continuing program for the economical and efficient management of the records of the agency.”¹² This policy guidance implements the requirements of the Act by codifying I&A's RIM program and outlining guidance for I&A personnel to effectively and efficiently manage federal records.

(ii) Per 36 C.F.R. § 1220.10, the National Archives and Records Administration (NARA) and the General Services Administration (GSA) share responsibility for overseeing records management throughout the government while agencies are responsible for establishing and maintaining a records management program that complies with NARA and GSA regulations and guidance.

(iii) All I&A personnel must comply with the requirements of this policy. Failure to comply with the requirements herein could lead to internal administrative actions or penalties (fine or imprisonment) (or some combination thereof).¹³

(b) General Principles.

(i) All federal records—temporary and permanent—will be managed electronically to the fullest extent possible per Office of Management and Budget (OMB)/NARA

¹¹ 44 U.S.C. § 3101.

¹² *Id.* § 3102.

¹³ 18 U.S.C. §§ 641, 2071.

Memorandum No. M-19-21, *Transition to Electronic Records* (June 28, 2019), and OMB/NARA No. M-23-07, *Update to Transition to Electronic Records* (Dec. 23, 2022).

(ii) Electronic transfers and records accessioned to NARA will be regulated by and in accordance with 36 C.F.R., Chapter XII, Subchapter B.

(iii) All records generated during a person's employment are the property of the Department of Homeland Security (DHS) and I&A. I&A personnel cannot use any outside email system to conduct official DHS business. If during an emergency a non-DHS email system is used, the employee is responsible for ensuring that any email records and attachments are saved in I&A's determined official records location (records shared drive, collaboration platform, etc.) within the employee's respective office, directorate, mission center, or equivalent unit within I&A's environment.

(iv) I&A must create, maintain, use, and dispose of records, non-records, and personal files as appropriate and in accordance with DHS Directive No. 141-01, *Records and Information Management* (as amended Sept. 26, 2019), and DHS Instruction No. 141-01-001, *Records and Information Management* (as amended Sept. 9, 2019), as well as any other legal or policy requirements and procedures.

(v) I&A offices must maintain a records inventory listing (RIL), office file plan (OFP), and essential records inventory form (ERIF), if applicable, to identify the records being managed within their respective area. I&A offices must have an appointed records liaison or records custodian (or both) to create and maintain that RIL, OFP, and ERIF, if applicable. Appointed records liaisons and records custodians are required to provide a RIL, OFP, and ERIF, if applicable, to the I&A Records and Information Management program annually in response to the DHS Chief Data Officer Directorate (CDOD) Executive Secretariat and DHS RIM Division data call taskers distributed throughout the Department.

(vi) I&A personnel shall successfully complete the DHS HQ mandatory Records Management online training session within 30 days of onboarding and annually thereafter.

(vii) I&A personnel are prohibited from destroying federal records, without an approved records schedule, regardless of record type or format and regardless of whether those records are categorized as temporary or permanent.

(c) Records and Information Management Program.

(i) The I&A Records Manager, appointed by the Deputy Under Secretary for Management, serves as the component lead on RIM-related matters and is responsible for managing I&A's RIM Program. The I&A Records Manager conducts the following:

- (A) In accordance with DHS Federal Emergency Management Federal Continuity Directive 1, implements the essential records program, conducts annual inspections, and records any information management requirements or report activities;
 - (B) Manages I&A records schedules, RILs, OFPs, ERIFs, and compliance reviews, and acts as the central point of contact for records liaisons;
 - (C) Coordinates approval of records schedules, transfers of permanent records, and storage of records with the DHS Records Officer;
 - (D) Ensures that the appropriate number of records liaisons and records custodians are designated across I&A, requesting additional designations and subject matter experts to assist appointed points of contact from I&A leadership as needed;
 - (E) Ensures records liaison and records custodian training is completed by designated records liaisons/records custodians within 30 days of appointment, and that annual records training is incorporated into I&A contracts, as appropriate;
 - (F) Develops an I&A-wide records management performance goal each year for both records liaisons and records custodians;
 - (G) Completes the NARA Records Management Training Online Sessions (levels one to three) within 120 days of assuming the position as the I&A Records Manager;
 - (H) Serves as I&A's representative on the DHS Records Management Council and the Intelligence Community Records Management Subcommittee;
 - (I) Provides exit briefings for all I&A personnel (including government employees, contractors, and detailees); and
 - (J) Provides guidance on digitization standards for I&A records.
- (d) Requirements for and Responsibilities of Records Custodians and Records Liaisons.
- (i) Each directorate, center, or division director (Approving Official) designates a records liaison for their directorate, center, or division (collectively, covered units) and a records custodian for each of their respective branches. For the I&A Front Office, which has no covered units, the heads of the program offices and the Deputy Chief of Staff are the Approving Officials for their program offices and those front office staff not in a program office, respectively.
 - (ii) The I&A Records Manager ensures that all designated records custodians and records liaisons attend the necessary records management training, led by the I&A RIM program, no later than 30 days from the date decided by the Approving Official.

(iii) When a current records custodian or records liaison transitions out of a division or mission center or branch, a new records custodian or records liaison will be designated within 30 days by the Approving Official.

(iv) Records liaisons within each I&A covered unit are the primary RIM points of contact for all designated records custodians under their purview. Records liaisons conduct the following:

(A) Provide guidance to I&A personnel about RIM issues, policies, and requirements within their respective offices and functional areas;

(B) Ensure that their respective office records are set up and maintained according to the NARA General Records Schedule, DHS HQ Records Schedules, or I&A Records Schedules; and

(C) Participate in the annual mandatory Records Manager assessments and provide an essential records inventory status report, if applicable, to the I&A Records Manager.

(v) Records custodians create, maintain, and dispose of records according to a designated NARA General Records Schedule, DHS HQ Records Schedules, or I&A Records Schedules. Records custodians do the following:

(A) Inform their records liaison of any issues regarding the records in their custody, such as the unauthorized deletion or loss of a record;

(B) Ensure the proper retention of records, non-records, and personal files subject to a legal hold or records freeze upon notification from the I&A RIM program on behalf of the Office of the General Counsel; and

(C) Participate in the annual mandatory I&A Records Manager assessments.

(vi) Records custodians and records liaisons maintain a RIL, OFP, and ERIF, if applicable, to identify the records being managed within their respective area. Records custodians and records liaisons provide these materials annually to the I&A RIM Program in support of the DHS CDOD Executive Secretariat data call taskers distributed throughout DHS.

(vii) Records custodians and records liaisons conduct shared drive management—which includes managing file storage, setting up filing structure, enforcing naming conventions, and ensuring that all permanent and temporary records are accompanied by finding aids and are in an acceptable file format per NARA standards.

(e) Responsibilities of I&A Personnel.

(i) To ensure proper records management across the organization, I&A personnel conduct the following:

- (A) Adequately document the organization, function, policies, decisions, procedures, and essential transactions of I&A and properly identify, capture, retain, label, and file records, regardless of form or format and regardless of what stage the record is at in the records management lifecycle;
- (B) Follow the disposition instructions for records schedule items identified in the NARA General Records Schedule, DHS HQ Records Schedules, and I&A Records Schedules;
- (C) Successfully complete the DHS mandatory records management online training within 30 days of onboarding and annually thereafter;
- (D) Coordinate records and information management activities with the records custodians and records liaisons designated for their covered unit within I&A to ensure compliance with RIM laws, policies, and procedures;
- (E) Create and maintain records and information consistent with the guidance of the records liaison and records custodian designated for their covered unit within I&A, both when operating in person and when teleworking;
- (F) Ensure any federal records under their direct control are transferred to their supervisors or records custodians assigned to their covered unit within I&A as part of offboarding from I&A;
- (G) Preserve and protect I&A records by notifying their respective records custodian, records liaison, and the I&A RIM program of any record violations apparently motivated by an intent to unlawfully remove, destroy, alter, or eliminate records; and
- (H) Identify the retention cutoff of temporary records eligible for destruction.

Prior to destruction, I&A personnel must have an approved receipt of record destruction by their respective Approving Official and the I&A RIM program documented in I&A Form 102-A, *Electronic Records Disposition Authorization Form*.

5-108: Restrictions on Post-Government Employment

This section is a placeholder. The policy will be included in a future version of the Policy Manual.

5-201: Planning, Procuring, and Managing Information Technology Resources

This Section of the Policy Manual establishes the responsibilities, requirements, and procedures for planning, procuring and managing Information Technology (IT) resources in accordance with applicable law and policy.

(a) Overview.

(i) This policy applies to all I&A personnel, including contractors supporting I&A, and employees detailed from other agencies to the Office of Intelligence and Analysis or other government personnel acting for I&A.

(ii) The Under Secretary for Intelligence and Analysis (USIA) has designated the Director of the Technology and Data Services Directorate (D/TDS) as the authorized I&A official responsible for exercising leadership and authority over I&A IT policies, programs, services, solutions, and resources. The USIA reviews and approves the I&A IT strategic plan, investment roadmap, and annual spend plan.

The D/TDS is required by law and Department of Homeland Security (DHS) policy to participate in all decisions related to planning, procuring, and managing IT resources. I&A plans, procures, and manages IT resources through the planning, programming, budgeting, and execution (PPBE) process, ensuring I&A's critical information systems effectively support mission operations.

(b) Planning IT Resources.

(i) I&A offices, program offices, directorates, centers, and divisions (covered units) include the D/TDS in planning and program development, including development of resource requests and proposals, for programs that involve IT resources.

(ii) During the planning phase of PPBE, the D/TDS works with internal and external stakeholders and the I&A Senior Staff (Chief of Staff; Deputy Under Secretaries for Analysis, Partnerships, Management, and Collection; Executive Director for the Intelligence Enterprise Program Office; and Director of the Transparency and Oversight Program Office) to—

(A) Determine a limited number of immediate IT operational goals for the upcoming fiscal year as well as broader, longer-term goals for future years;

(B) Identify and communicate long-term IT strategies to guide operational activities, resource planning, and analytic activities to inform near and longer-term resource decisions;

(C) Develop the strategic priorities and IT resources planning priorities for the future years' budget;

- (D) Contribute to I&A resource planning guidance to inform subsequent IT programming and budgeting phases;
 - (E) Review, assess, and validate projected IT implementation risks (i.e., cost, schedule, and performance) and advise the USIA, Principal Deputy Under Secretary for Intelligence and Analysis (PDUSIA), and Senior Staff (collectively, Senior Leadership) on mitigation strategies.
- (iii) During the programming phase of PPBE, the D/TDS works with internal and external stakeholders and Senior Leadership to—
- (A) Allocate IT resources to organizational goals and objectives and establish priorities and performance measures based on leadership guidance, including, but not limited to, strategic plans, and resource planning proposals;
 - (B) Align IT strategic priorities and budget resources to the fiscal guidance provided by the Office of the Director of National Intelligence (ODNI), DHS, and I&A;
 - (C) Provide IT resource requirements to the Director of the Financial Resources Management Division (D/FRM) for the annual Resource Allocation Plan submission; and
 - (D) Review and approve the IT elements of any acquisition plans through the I&A Information Technology Acquisition Review process.
- (c) Procuring IT Resources.
- (i) During budget formulation, the D/TDS works with internal and external stakeholders and Senior Leadership to—
- (A) Review the results of the DHS Resource Allocation Decision to identify proposed IT budget estimates for the upcoming budget year plus four fiscal years for submission in the budget justification;
 - (B) Review the results of the RAD to identify the proposed IT budget estimates for the upcoming budget year plus four fiscal years submitted in the Intelligence Program Budget Submission to the ODNI Chief Financial Officer;
 - (C) Conduct a multi-year evaluation (e.g., independent government cost estimate) to validate projected requirements and develop detailed IT estimates;
 - (D) Develop fully justified one-year IT budget submissions for inclusion in the Congressional Justification Book and Congressional Budget Justification Book;
 - (E) Participate in program reviews with designated financial and performance management personnel;

- (F) Include program changes highlighted in the President's Budget Request in alignment with the I&A Strategic Plan and IT Acquisition Strategy;
 - (G) Approve requests for reimbursable funding;
 - (H) Develop an I&A spend plan, which includes an operations and maintenance budget; and
 - (I) Establish systems engineering life cycle (SELC) activities and ensure that IT spending (including hidden IT) is aligned with DHS and I&A strategies, and review and approve, in consultation with the DHS Office of Program Accountability and Risk Management, SELC tailoring plans for major IT acquisition programs.
- (ii) During the year of budget execution, the D/TDS works in consultation with internal and external stakeholders and Senior Leadership to responsibly expend IT resources.
- (A) Covered units ensure that all IT purchase requests correspond to an approved IT spend plan. The D/FRM verifies all IT purchase requests against the approved IT spend plan prior to certifying funds.
 - (B) The D/TDS documents and reports obligated and expended funds and assesses those results for incorporation into future program plans.
- (d) Managing IT Resources.
- (i) The D/TDS works in coordination with Senior Leadership and the Program and Performance Evaluation Division within the Office of Management to assess the effectiveness of I&A IT programs, activities, initiatives, and investments by analyzing financial information along with evidence of programmatic progress during the current fiscal year and comparing progress with I&A strategies and objectives.
 - (ii) The D/TDS performs I&A strategic mid-year reviews to assess IT program performance and works with the D/FRM to redistribute funds under specific statutory authorities to reprogram or transfer funds from one activity to another.
 - (iii) The D/TDS produces an end-of-year review for Senior Leadership to summarize activities, milestones, and accomplishments.
 - (iv) The D/TDS produces and provides reports to DHS and ODNI, as required.

5-202: Responsible Framework for Use of Artificial Intelligence and Machine Learning

This section is a placeholder. The policy will be included in a future version of the Policy Manual.

5-203: Use of Commercially Available Information

As corporations increasingly aggregate information from the devices and applications used by the public every day, the commercially available information (CAI) they generate can reveal potentially sensitive details and activities, often without the awareness or consent of the individuals whose information can be revealed. CAI is any data or other information that is of a type customarily made available and sold, leased, or licensed to the general public or non-governmental entities for purposes other than governmental purposes. It includes data and information for exclusive government use, knowingly and voluntarily provided by, made accessible by, or procured from corporate entities at the request of a government entity, or on their own initiative. As such, CAI does not include information obtained through compulsory processes, such as court orders or directives under the Foreign Intelligence Surveillance Act. The U.S. Government and private entities can lawfully purchase or obtain access to a variety of CAI for diverse applications, and the Office of Intelligence and Analysis (I&A) currently relies on a small number of these products to support its intelligence missions.

I&A personnel are authorized to use CAI consistent with the guidance below. All I&A intelligence activities involving CAI are conducted in accordance with the Constitution, the laws of the United States, presidential guidance, regulation, and national, departmental, and I&A policy, including I&A's Intelligence Oversight Guidelines.

(a) General Principles. The principles listed below govern I&A's access to, and collection, retention, and processing of CAI.

(i) I&A limits its access to "Sensitive CAI," defined below, to the extent consistent with mission and administrative needs, employing the safeguards described in this policy guidance.

(A) CAI will be deemed Sensitive CAI if it 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), and is known or reasonably expected to contain—

(I) A substantial volume of identifying information about U.S. persons (U.S. Persons Information (USPI)); or

(II) A greater than *de minimis* volume of sensitive data concerning any person, or data revealing sensitive activities of any person.

(a.) Sensitive data captures personal attributes, conditions, or identifiers that are traceable to one or more specific person, either through the dataset itself or by correlating the dataset with other available information; and that concerns the person or 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 person or persons described by the data.

(b.) Sensitive activities are 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 person who engaged in the activity.

(B) Sensitive CAI does not include 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 limited data samples used to evaluate whether to purchase the full dataset.¹⁴

(ii) The protection of privacy, civil rights, and civil liberties is an integral consideration in determining the parameters for accessing, collecting, and processing CAI. Accordingly, I&A will undertake to prioritize funding for privacy enhancing methods and technologies to facilitate access control, auditing, retention, destruction, and oversight requirements.

(iii) In the interest of information sharing and transparency, I&A will provide information to other Intelligence Community elements, DHS components, relevant oversight entities, and the public on the policies and procedures governing its access to, and collection and processing of, CAI, consistent with the protection of sources and methods, law enforcement sensitive information, and other privileged or operationally sensitive information.

¹⁴ If sample data is used for any purpose beyond evaluation for purchase, including for anything that constitutes an intelligence activity, it is subject to the protections and procedures outlined in this memorandum.

(b) Procurement.

(i) CAI is procured through the Contracting Officer in the Acquisitions Branch of the Office of Management's Financial Resource Management Division (FRM/Acquisitions).¹⁵

(ii) FRM/Acquisitions assists in identifying potential CAI procurement and alerts the Privacy and Intelligence Oversight Officer to any potential procurement of CAI. Any information procured from a commercial provider is reviewed by the Privacy and Intelligence Oversight Officer and the Chief Data Officer (CDO) to determine whether it is CAI.

(iii) Each procurement requires written authorization from the Privacy and Intelligence Oversight Officer and the CDO, and in the case of Sensitive CAI, from the Under Secretary for Intelligence and Analysis (USIA) or their designees, described below.

(A) The Deputy Under Secretary for Management (DUS/M) and the Director of the Transparency and Oversight Program Office (D/TOPO) may jointly approve Sensitive CAI procurement on behalf of the USIA.

(B) DUS/M and D/TOPO will report to the USIA any acquisitions of Sensitive CAI.

(iv) I&A personnel are prohibited from using CAI obtained in their personal capacity, or any CAI not approved through the processes outlined in this section, for any government purposes.

(c) Initial Assessment and Sensitivity. Before new CAI can be procured by I&A, the information will be subject to a written assessment conducted jointly by the Privacy and Intelligence Oversight Officer and CDO in coordination with the office that wishes to access or collect the CAI. If the CAI experiences a material change in use, a new assessment must be completed. This assessment will include—

(i) An evaluation of the CAI's quality, integrity, and potential bias;

(ii) A determination as to whether the CAI furthers an authorized intelligence mission or administrative need, including I&A's legal authority to procure the CAI, guided by the nature, scope, reliability, and timeliness of the dataset required to fill the relevant requirement;

¹⁵ We use the term "procure" throughout this memorandum to refer to the purchase (or use of free trials) of either access to, or possession or control over, CAI.

(iii) Reasonable efforts to determine the original source and aggregation or generation methods of the CAI;

(iv) A review of any licensing agreements or contract restrictions; and

(v) A determination as to whether the information or data should be considered Sensitive CAI. I&A will notify the Office of the Director of National Intelligence (ODNI) if the Privacy and Intelligence Oversight Officer and the CDO determine specific CAI is not Sensitive if I&A is aware another Intelligence Community element determined the same or similar CAI is Sensitive.

(d) Sensitive CAI Assessment.

(i) If CAI is determined to be Sensitive CAI, the CAI Assessment will also include the following:

(A) A determination by the Privacy and Intelligence Oversight Officer as to whether the CAI contains sensitive data or describes sensitive activities, as described in Section 5-203(a)(i)(A)(II) above, and a description of the specific sensitivities, if so.

(B) The privacy, civil rights, and civil liberties risks associated with the CAI along with the impact of privacy-enhancing techniques and safeguards to mitigate those risks such as filtering or anonymizing data, limiting access and retention, differential privacy techniques, or masking sensitive information; and

(C) In consultation with the Director of the Counterintelligence Program Division and the I&A Chief Information Security Officer in the Office of Management's Technology and Data Services Directorate, the security, operational, and counterintelligence risks associated with the CAI along with strategies to mitigate those risks.¹⁶

(ii) Upon completion of the Sensitive CAI Assessment, the Privacy and Intelligence Oversight Officer and CDO will provide their findings to the DUS/M and D/TOPO with a recommendation as to whether acquisition of the CAI is appropriate and sufficiently justified. This recommendation will include the specific privacy enhancing technologies, how the CAI will be accessed and controlled, and any measures necessary to mitigate security and privacy risks. Prior to the procurement of Sensitive CAI, the DUS/M and D/TOPO must jointly review the recommendation, approve the access, document the determination in writing, and notify the USIA of their joint determination.

¹⁶ I&A will, to the extent the information is reasonably available to it, consider whether any other Intelligence Community element previously accessed or collected the same or similar Sensitive CAI.

(iii) I&A need not conduct an assessment of CAI under the following circumstances:

(A) If another Intelligence Community element has shared its most recent documented evaluation of a particular collection of CAI, I&A may rely on the factual findings set forth in the other element's assessment so long as I&A documents those findings; or

(B) Where the USIA determines that exigent circumstances require a temporary waiver of the assessment, provided that the Privacy and Intelligence Oversight Officer and CDO document the justification for doing so and conduct the assessment promptly after the exigent circumstance passes.

(iv) Even where a Sensitive CAI Assessment is not required pursuant to one or both of the exceptions listed in Section 5-203(d)(iii) above, procurement of Sensitive CAI still requires DUS/M and D/TOPO approval.

(e) Periodic Review. All CAI will be reviewed jointly by the CDO and Privacy and Intelligence Oversight Officer using the criteria set forth in Section 5-203(c) above at least once per year, or upon a material change to the current assessment, to assess its relevance to mission or administrative needs, the adequacy of its safeguards, and whether it should continue to be retained. Sensitive CAI used by I&A will be reviewed in this fashion at least twice per year. The CDO and Privacy and Intelligence Oversight Officer will produce a report detailing the findings of these reviews as they are completed.

(f) Retention Requirements.

(i) Where I&A not only accesses, but also procures CAI, that information must be safeguarded at a level that is appropriate to its sensitivity, generally determined by its anticipated use and the volume, proportion, and nature of USPI.

(ii) Systems containing Sensitive CAI must enable I&A to implement, manage and audit privacy and civil liberties protections.

(iii) I&A must apply security and privacy controls to protect USPI and reduce privacy risks to individuals when accessing, collecting, and processing CAI. These safeguards include the creation and implementation of a "Moderate Privacy Overlay" control set for any Sensitive CAI retained on an I&A or other National Security System.

(iv) Contractors operating systems with Sensitive CAI must have an authority to operate. Those systems should implement the applicable privacy control baseline as defined in Intelligence Community Directive 503, *Intelligence Community Information Technology Systems Security Risk Management, Certification, and Accreditation* (Oct. 25, 2024), and

Committee on National Security Systems Instruction No. 1253, *Security Categorization and Control Selection and Control Selection for National Security Systems* (March 27, 2014).

(g) Enhanced Safeguards. Sensitive CAI may require enhanced safeguards to mitigate the risks identified in the assessment described in Section 5-203(d). Such safeguards may include one or more of the following measures:

(i) Procedures to restrict access, including limiting the number of personnel with access and putting in place access controls;

(ii) 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;

(iii) A requirement to provide written justification and obtain the approval of a senior executive or other senior leader prior to undertaking any queries, searches or correlations of Sensitive CAI that are intended to return known USPI, or reasonably likely to return a substantial volume of USPI;

(iv) Procedures to require the approval by a senior executive or other senior leader when conducting queries or other searches of Sensitive CAI that constitute data mining, meaning a program involving pattern-based queries, searches, or other analyses of one or more electronic databases, where—

(A) I&A is conducting the queries, searches, or other analyses to discover or locate a predictive pattern or anomaly indicative of terrorist or criminal activity on the part of any individual or individuals;

(B) The queries, searches, or other analyses are not subject-based and do not use personal identifiers of a specific individual, or inputs associated with a specific individual or group of individuals, to retrieve information from the database or databases; and

(C) The purpose of the queries, searches, or other analyses is not solely—

(I) The detection of fraud, waste, or abuse in a government agency or program; or

(II) The security of a government computer system;

(v) Procedures to restrict dissemination, including requiring higher level approval or legal review before or after USPI is disseminated;

(vi) Using privacy-enhancing techniques such as information masking that indicates the existence of USPI without providing the content of the information until the appropriate approvals are granted;

(vii) Procedures for deleting USPI 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; or

(viii) Additional protective measures or training.

(h) Data Management Plan. In coordination with the CDO, any subcomponent within I&A that wishes to procure CAI will develop a data management plan for each collection of Sensitive CAI from access, through the data lifecycle, to disposition, pursuant to I&A's data management policies.

(i) Documentation Requirements.

(i) The CDO will maintain records of all CAI, including the assessments and data management plans described above, and make this information available to other IC elements and ODNI.

(ii) For Sensitive CAI, the CDO will also document and maintain records of its recommendations, assessments, and any underlying documentation. The CDO will also track if I&A makes unevaluated data from a CAI dataset available to any other Intelligence Community element or foreign partner (and which partners).

(iii) The Privacy and Intelligence Oversight Officer will maintain a separate copy of the records described in Section 5-203(c)-(e) above.

(j) Sensitive CAI Requirements for Research and Development. Information that otherwise qualifies as Sensitive CAI is exempt from the requirements outlined in Sections 5-203(d)-(h) if the Privacy and Intelligence Oversight Officer and CDO determine the information will be used solely for research and development purposes. If such use cases arise, the DUS/M and the D/TOPO will establish an institutional review board to provide oversight of CAI for research and development purposes. The Privacy and Intelligence Oversight Officer will also notify the DHS Office of the General Counsel, the DHS Privacy Office, the DHS Office for Civil Rights and Civil Liberties, ODNI Office of General Counsel, and the ODNI Civil Liberties, Privacy, and Transparency Office prior to the procurement of CAI in this manner.

5-301: Career Development

This section is a placeholder. The policy will be included in a future version of the Policy Manual.

Enclosure 1 –References

This section is a placeholder. A references section will be included in a future version of the Policy Manual.

Enclosure 2 – Acronyms

Abbreviation	Definition
AAD	Analytic Advancement Division
AGC/Intel	Associate General Counsel for Intelligence
AWOL	Absence Without Leave
AWS	Alternative Work Schedule
CAI	Commercially Available Information
CAL	Component Audit Liaison
CATT	Correspondence Analyst Tracking Tool
CBP	Customs and Border Protection
CDO	Chief Data Officer
CDOD	Chief Data Officer Directorate
CFO	Chief Finance Officer
CFR	Code of Federal Regulations
CIC	Cyber Intelligence Mission Center
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CRCL	Office for Civil Rights and Civil Liberties
CTC	Counterterrorism Mission Center
D/AAD	Director of the Analytic Advancement Division
D/TOPO	Director of the Transparency and Oversight Program Office
D/WME	Director of Workforce Management and Engagement
DAL	Departmental Audit Liaison
DTW	Duty to Warn
DUS/A	Deputy Under Secretary for Analysis
DUS/C	Deputy Under Secretary for Collection
DUS/M	Deputy Under Secretary for Management
DUS/P	Deputy Under Secretary for Partnerships
EEO	Equal Employment Opportunity
ELO	Engagement, Liaison, and Outreach Division
FBI	Federal Bureau of Investigation
FID	Field Intelligence Division
FIP	Field Intelligence Program
FIPP	Fair Information Practice Principle
FIR	Field Intelligence Report

FOIA	Freedom of Information Act
FSLTTP	Federal, State, Local, Tribal, Territorial, and Private Sector
FWS	Flexible Work Schedule
GAO	Government Accountability Office
GFE	Government Furnished Equipment
GSA	General Services Administration
I&A	Office of Intelligence and Analysis
I&A Exec Sec	Office of Intelligence and Analysis Executive Secretariat
I&A Ombuds	I&A Organizational Ombuds
IC	Intelligence Community
ICD	Intelligence Community Directive
ICE	Immigration and Customs Enforcement
ICP	Internal Controls Program
IEPO	Intelligence Enterprise Program Office
IIR	Intelligence Information Report
IOO	Intelligence Oversight Officer
IPA	Intergovernmental Personnel Act of 1970
IT	Information Technology
ITA	Intelligence Training Academy
IWC	Intelligence Watch and Coordination Center
JDPO	Joint Duty Program Office
KPP	Key Processes and Products
LNO	Liaison Officer
MHS	Migration and Human Smuggling
MOA	Memorandum of Agreement
NARA	National Archives and Records Administration
NIP	National Intelligence Program
NST	Nation-State Threat Mission Center
ODNI	Office of the Director of National Intelligence
ODNI/PAO	Office of the Director of National Intelligence Public Affairs Office
OFF	Office File Plan
OGC	Office of the General Council
OGC/ILD	Office of the General Council Intelligence Law Division
OMB	Office of Management and Budget
OPSPRO	Operational Proposal

OSAC	Overseas Advisory Council
OSID	Open Source Intelligence Division
PCOB	Policy Coordination and Oversight Branch
PCLOB	Privacy and Civil Liberties Oversight Board
PDUSIA	Principal Deputy Under Secretary for Intelligence and Analysis
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PIOB	Privacy and Intelligence Oversight Branch
PMB	Personnel Management Board
PPBE	Planning, Programming, Budgeting, and Execution
PRIV	Privacy Office
PTA	Privacy Threshold Analysis
RAD	Resource Allocation Division
RC	Records Custodian
RIL	Records Inventory Listing
RIM	Records and Information Management
RL	Records Liaison
RLNO	Resident Liaison Officer
RM&A ICOFR	Risk Management and Assurance Internal Controls Over Financial Reporting
RSB	Recruitment and Selection Board
SCAO	Senior Component Accountable Official
SCI	Sensitive Compartmented Information
SES	Senior Executive Service
TBS	Transborder Security Mission Center
TDB	Talent and Development Branch
TDS	Technology and Data Services
TOC	Transnational Organized Crime
TOPO	Transparency and Oversight Program Office
USIA	Under Secretary for Intelligence and Analysis
USPI	United States Persons Information
WM&E	Workforce Management and Engagement

Enclosure 3 – I&A Lexicon

- **Chief Intelligence Officer (CINT):** The DHS official who exercises leadership and authority over intelligence policy and programs throughout the Department and acting in conjunction with, and without preempting the authorities of, the DHS Chief Information Officer and the DHS Chief Security Officer, exercises leadership and authority over information sharing and safeguarding policy and programs throughout the Department. The CINT also provides strategic oversight to and supports the missions and goals of members of the DHS Intelligence Enterprise. This person is designated in statute and in departmental policy as the Under Secretary for Intelligence and Analysis. [Source: DHS Instruction 264-01-001]
- **Classified Information:** Information that has been determined pursuant to Executive Order 13526 or any predecessor order to require protection against unauthorized disclosure. [Source: DHS Lexicon]
- **Collection:** Obtaining or acquiring information from outside the Intelligence Community (including from the Office of the Secretary and other Components) by any means, including, but not limited to, information that is volunteered, and regardless of whether the information is temporarily or permanently retained. Information that only momentarily passes through an I&A computer system is not collected. Collection is distinct from access to information in that collection requires that the information be copied, saved, or used in some manner, including, but not limited to, information that is copied or saved in the form of summaries, reports, or notes, whereas information that is accessed is merely viewed or examined, but is not collected even if it is transmitted on an I&A information technology system. [Source: I&A Intelligence Oversight Guidelines, Glossary]
- **Contact [Communication]:** All manner of personal or impersonal communication that includes, but is not limited to, written, telephonic, electronic mail, text messaging, chat room discussion, facsimile, wire, and/or amateur radio. [Source: DHS Lexicon]
- **Counterintelligence:** Information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, or persons, or their agents, or international terrorist organizations or activities. [Source: I&A Intelligence Oversight Guidelines, Glossary]
- **Critical Infrastructure:** Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on the Nation's economic security, public health, public safety, or any

combination of those matters. [Source: I&A Intelligence Oversight Guidelines, Glossary]

- **DHS Intelligence Enterprise (DHS-IE):** The primary mechanism for the integration and management of the Department’s intelligence programs, projects, and activities, led by the Chief Intelligence Officer and consisting of the Component Intelligence Programs of DHS Intelligence Components. The primary function of the DHS Intelligence Enterprise is to coordinate and deconflict the National and Departmental Intelligence Functions of the Department in support of the unified collection, gathering, processing, analysis, production, and dissemination of National and Departmental Intelligence both within the Department and in providing support to the Homeland Security Enterprise. [Source: DHS Instruction 264-01-001]
- **Dissemination:** The transmission, communication, sharing, or passing of intelligence or information outside I&A by any means, including oral, electronic, or physical means. Dissemination therefore includes providing any access to information retained by I&A to persons outside I&A. [Source: I&A Intelligence Oversight Guidelines, Glossary]
- **Duty to Warn:** The requirement to warn U.S. and non-U.S. person(s) of impending threats of intentional killing, serious bodily injury, or kidnapping. [Source: IA-105]
- **Foreign Intelligence:** Information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, foreign persons, or international terrorists. [Source: I&A Intelligence Oversight Guidelines, Glossary]
- **I&A Finished Intelligence Product:** The physical manifestation, regardless of form or format, of analytic efforts conducted in furtherance of the I&A mission, which represent the analytic assessment, judgment, or other analytic input of I&A or intelligence personnel, are required to comply with ICD 203, and are intended to be disseminated outside of DHS. [Source: IA-901]
- **Intelligence Community (IC):** The United States Intelligence Community as defined at Title 50, United States Code, Section 3003, “Definitions,” and Section 3.5(h) of Executive Order 12,333, “United States Intelligence Activities,” as amended July 30, 2008. [Source: I&A Intelligence Oversight Guidelines, Glossary]
- **Intelligence Information:** Analyzed and synthesized information that is of tactical, operational, or strategic value. It includes foreign intelligence and counterintelligence, as defined by Executive Order 12,333, December 4, 1981, as amended, or by a successor order. [Source: DHS Lexicon]
- **Key Resources:** Publicly or privately controlled resources essential to the minimal

operations of the economy and government. [Source: I&A Intelligence Oversight Guidelines, Glossary]

- **Personally Identifiable Information (PII):** Any information that permits the identity of an individual to be directly or indirectly inferred, including any other information that is linked or linkable to that individual. This definition applies regardless of whether the individual is a United States citizen, legal permanent resident, visitor to the United States, DHS employee, or contractor. [Sources: DHS Lexicon, DHS Instruction 262-05-001]
- **Publicly Available Information (PAI):** Information that has been published or broadcast for public consumption, is available on request to the public, is accessible on-line or otherwise to the public, is available to the public by subscription or purchase, could be seen or heard by a casual observer, is made available at a meeting open to the public, or is obtained by visiting any place or attending any event open to the public. Social media sites, Internet sites, chat rooms, bulletin boards, and other electronic and other fora, or portions of the same, belonging to individuals or groups that limit access by use of criteria that cannot generally be satisfied by members of the public are not publicly available sources. [Source: I&A Intelligence Oversight Guidelines, Glossary]
- **Reasonable Belief:** A belief based on facts and circumstances such that a reasonable person would hold that belief. A reasonable belief must rest on facts and circumstances that can be articulated; “hunches” or intuitions are not sufficient. A reasonable belief can be based on experience, training, and knowledge as applied to particular facts and circumstances, and a trained and experienced intelligence professional can hold a reasonable belief that is sufficient to satisfy these criteria when someone lacking such training or experience would not hold such a belief. [Source: I&A Intelligence Oversight Guidelines, Glossary]
- **Records:** All books, papers, maps, photographs, machine readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by an agency of the United States Government under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the Government or because of the informational value of the data in these documentary materials. A record may also be any item, collection, or grouping of information about an individual that is maintained by an agency. [Sources: DHS Instruction 262-05-001, IA-102]
- **Records Management (RM):** The planning, controlling, directing, organizing, training, promoting, and other managerial activities involved with respect to records creation, records maintenance and use, and records disposition to achieve adequate and proper

documentation of the policies and transactions of the Federal Government and effective and economical management of agency operations. [Source: 44 U.S.C. § 2901]

- **Terrorism:** Any activity that (1) involves an act that (a) is dangerous to human life or potentially destructive of critical infrastructure or key resources; and (b) is a violation of the criminal laws of the United States or of any State or other subdivision of the United States; and (2) appears to be intended (a) to intimidate or coerce a civilian population; (b) to influence the policy of a government by intimidation or coercion; or (c) to affect the conduct of a government by mass destruction, assassination, or kidnapping. [Source: I&A Intelligence Oversight Guidelines, Glossary]
- **United States Person (USPER):** (1) A United States citizen, (2) an alien known by I&A to be a permanent resident alien (i.e., lawful permanent resident), (3) an unincorporated association substantially composed of United States citizens or permanent resident aliens, or (4) a corporation incorporated in the United States, except for a corporation directed and controlled by a foreign government or governments. In determining whether an unincorporated association affiliated with a foreign-based international organization is substantially composed of United States citizens or permanent resident aliens, the membership of the entire international organization is considered if the association operates directly under the control of the international organization and has no independent program or activities in the United States, but only the membership of the organization within the United States is considered if the organization within the United States conducts programs or engages in activities separate from or in addition to those directed by the international affiliate. [Source: I&A Intelligence Oversight Guidelines, Glossary]
- **United States Person Information (USPI):** Information that is reasonably likely to identify one or more specific United States Persons. USPI may be either a single item of information or information that, when combined with other available information, is reasonably likely to identify one or more specific United States Persons. Determining whether information is reasonably likely to identify one or more specific United States Persons requires a case-by-case assessment by a trained intelligence professional. It is not limited to any single category of information or technology. [Source: I&A Intelligence Oversight Guidelines, Glossary]



Homeland
Security

UNCLASSIFIED



Department of Homeland Security
Office of Intelligence and Analysis
Intelligence Oversight Guidelines

UNCLASSIFIED

Table of Contents

INTRODUCTION 1

1. GENERAL PROVISIONS 2

 1.1. AUTHORIZED INTELLIGENCE MISSIONS 3

 1.1.1. National Missions 3

 1.1.2. Departmental Missions 3

 1.2. GENERAL PROTECTIONS FOR UNITED STATES PERSONS INFORMATION 4

 1.3. REQUIRED CONSULTATION 5

2. GUIDELINES FOR COLLECTION, RETENTION, AND DISSEMINATION 6

 2.1. COLLECTION 6

 2.1.1. Collection Method (Overtly or through Publicly Available Sources) 6

 2.1.2. Collection Techniques (Least Intrusive Means) 6

 2.1.3. Collection of USPI 8

 2.2. RETENTION 9

 2.2.1. Retention for Evaluation 10

 2.2.2. Permanent Retention 10

 2.2.3. Information Categories 11

 2.2.4. Additional Requirements for Certain Communications 15

 2.3. DISSEMINATION 15

 2.3.1. General Dissemination Requirements 15

 2.3.2. Dissemination of Unevaluated Information within the Intelligence Community 16

 2.3.3. Dissemination with Approval 17

 2.3.4. Additional Requirements for Foreign Disseminations 17

 2.3.5. Anonymization Requirement 17

3. SPECIAL GUIDELINES FOR BULK DATA TRANSFERS 17

 3.1. BULK DATA COLLECTION 19

 3.2. RETENTION OF BULK DATA COLLECTIONS 21

 3.3. BULK DATA DISSEMINATIONS 22

4. GUIDELINES FOR OTHER ACTIVITIES 23

 4.1. PARTICIPATION IN ORGANIZATIONS WITHIN THE UNITED STATES 23

 4.1.1. Conduct Rising to the Level of Participation 23

 4.1.2. Participation on Behalf of I&A 24

UNCLASSIFIED

4.1.3. Participation in a Personal Capacity 26

4.2. ASSISTANCE TO LAW ENFORCEMENT AND OTHER CIVIL AUTHORITIES 26

4.3. REQUESTS FOR ASSISTANCE 27

4.4. SHARED REPOSITORIES 27

5. MISCELLANEOUS PROVISIONS 28

5.1. EFFECTIVE DATE 28

5.2. INTERPRETATION 28

5.3. DEPARTURES 28

5.4. AMENDMENTS 29

5.5. DELEGATION 30

GLOSSARY OF DEFINED TERMS Glossary-1

APPROVAL Approval-1

INTRODUCTION

The Department of Homeland Security Office of Intelligence and Analysis (I&A) is committed to delivering timely, actionable, predictive intelligence to its Federal, State, local, tribal, territorial, international, and private sector partners in support of the Department's national and homeland security missions. At the same time, these activities must be conducted in a manner that is consistent with all applicable requirements of the law, including the Constitution, and that appropriately protects individuals' privacy, civil rights, and civil liberties. Executive Order No. 12,333, updated most recently on July 30, 2008, requires all *Intelligence Community* elements, including I&A, to develop guidelines governing the *collection, retention, and dissemination* of information concerning *United States Persons* that are approved by the Attorney General after consultation with the Director of National Intelligence.* Separate provisions of the executive order require guidelines for other *intelligence activities* that also must be approved by the Attorney General.

The guidelines set forth below fulfill these requirements. They have been approved by the Attorney General after consultation with the Director of National Intelligence. Although many of the provisions of Executive Order No. 12,333 only apply to *United States Persons Information (USPI)*, as a matter of policy, DHS extends some of the guidelines' protections to all persons. The guidelines supersede the Memorandum from Charles E. Allen, Under Secretary for Intelligence and Analysis, and Matthew L. Kronisch, Associate General Counsel (Intelligence), Interim Intelligence Oversight Guidelines for the Office of Intelligence & Analysis (Apr. 3, 2008).

The guidelines are divided into five parts. Part One sets forth general provisions applicable to all I&A employees (including detailees or other Government personnel acting for I&A) and contractors supporting I&A (hereinafter "*I&A personnel*") in the conduct of their intelligence activities. Part Two establishes standard guidelines for the collection, retention, and dissemination of intelligence and information for intelligence purposes, while Part Three delineates separate, special guidelines for *bulk data transfers* containing USPI. Part Four concerns certain other activities conducted by I&A personnel, and Part Five contains miscellaneous provisions regarding the guidelines. A glossary of defined terms is attached to the document.

These guidelines ensure that I&A executes its vital mission to protect the Homeland without compromising the values essential to our national identity as a free people. They apply to all

* Defined terms are *italicized* when first used.

I&A personnel when engaging in intelligence activities on behalf of I&A. It is the responsibility of all I&A personnel to follow them.

1. GENERAL PROVISIONS

The guidelines set forth below apply to all I&A personnel engaging in any activity for an intelligence purpose, including, but not limited to, the collection, retention, and dissemination of intelligence and information. An activity is for an intelligence purpose where it is intended to inform the tactical, operational, or strategic decision making by national or departmental officials for national security, homeland security, border security, or law enforcement purposes. The guidelines do not apply to I&A personnel acquiring, maintaining, reviewing, or transferring intelligence or information for non-intelligence purposes, such as administrative purposes (e.g., information about systems administration, the performance of contractors, public affairs, correspondence files, personnel and training records, or training materials); internal or external oversight of I&A activities; crimes reporting not constituting a dissemination as authorized under section 2.3; or the retention, processing, or disclosure of information to members of the public pursuant to requests made under Title 5, United States Code, Section 552, "Freedom of Information Act," or Title 5, United States Code, Section 552a, "Privacy Act of 1974," or pursuant to civil or criminal discovery requests.

I&A personnel must abide by all applicable provisions and observe all applicable requirements and restrictions imposed by the Constitution, the provisions of Executive Order No. 12,333, the laws of the United States, applicable directives, and these guidelines. I&A personnel are prohibited under all circumstances from requesting any other person to engage in any conduct forbidden by these authorities. I&A personnel are prohibited under all circumstances from engaging in any intelligence activities, including the dissemination of information to the White House, for the purpose of affecting the political process in the United States, for the sole purpose of monitoring activities protected by the First Amendment or the lawful exercise of other rights secured by the Constitution or laws of the United States, or for the purpose of retaliating against a whistleblower or suppressing or burdening criticism or dissent. Further, as a matter of internal DHS policy, I&A personnel are not permitted to engage in intelligence activities based solely on an individual's or group's race, ethnicity, gender, religion, sexual orientation, gender identity, country of birth, or nationality. The use of these characteristics, in combination with other information, is permitted, where such use (1) is intended and reasonably believed to support one or more of the national or departmental missions described below in Section 1.1 and (2) is narrowly focused in support of that mission (or those missions). This does not otherwise limit the

authorized collection, retention, or dissemination of biographic information of specific individuals.

1.1. AUTHORIZED INTELLIGENCE MISSIONS

I&A personnel are authorized to engage in intelligence activities where they have a *reasonable belief* that the activity supports one or more of the national or departmental missions listed below. These missions reflect I&A's range of authorities and responsibilities as an element of the Intelligence Community and a component of the Department of Homeland Security, and are not exclusive of one another—I&A activities can be in furtherance of both national and departmental missions simultaneously.

1.1.1. National Missions

The intelligence activities of I&A personnel further a national mission where they assist the President or other executive branch officials performing executive functions in the development and conduct of foreign, defense, and economic policies or the protection of the United States national interests from foreign security threats, or, as appropriate, where they assist the Congress of the United States. Examples of foreign security threats include, but are not limited to, the following:

- a. *International terrorism* threats;
- b. The proliferation of weapons of mass destruction;
- c. Intelligence activities directed against the United States;
- d. International criminal drug activities; and
- e. Other hostile activities directed against the United States by *foreign powers*, organizations, persons, and their agents.

1.1.2. Departmental Missions

The intelligence activities of I&A personnel further a departmental mission where they assist the Department, other departments and agencies of the Federal Government, State and local government agencies and authorities, the private sector, or other entities in identifying protective and support measures regarding threats to homeland security, including, but not limited to:

UNCLASSIFIED

- a. *Domestic terrorism* threats;
- b. Threats to *critical infrastructure* and *key resources*;
- c. Significant threats to the Nation's economic security, public health, or public safety, including, but not limited to, local manifestations of national threats (e.g., local outbreaks of diseases reasonably likely to pose the risk of becoming a national pandemic);
- d. *Major disasters* and other catastrophic acts; and
- e. Any other threat of such severity and magnitude that effective response would be beyond the capabilities of any affected State and local governments, such that Federal assistance would be necessary.

In addition, the intelligence activities of I&A personnel further a departmental mission where they support the Secretary, the Deputy Secretary, the DHS Chief of Staff, or their respective staff, Component Heads, or any other departmental officials, offices, or elements in the execution of their lawful missions.

1.2. GENERAL PROTECTIONS FOR UNITED STATES PERSONS INFORMATION

I&A personnel must take reasonable steps to determine whether intelligence or information contains USPI at the point at which the intelligence or information is first obtained by I&A. A person within the United States is presumed to be a United States Person unless specific information to the contrary is obtained. A person outside the United States or whose location is unknown is presumed not to be a United States Person unless specific information to the contrary is obtained.

With respect to USPI, I&A personnel will only *access* and/or use USPI when they have appropriate security clearances, accesses, and a mission requirement (consistent with the missions set forth above at Section 1.1). Further, when retrieving information electronically, I&A personnel will tailor their queries or other techniques to the extent practicable to minimize the amount of USPI returned that is irrelevant to fulfilling the purpose of the query. To facilitate compliance with these requirements, I&A will:

UNCLASSIFIED

- a. Take reasonable steps to audit access to information systems containing USPI and periodically audit queries or other search terms to assess compliance with these guidelines;
- b. As practicable, establish written procedures to document the basis for conducting a query of unevaluated information that is intended to reveal USPI;
- c. Take reasonable steps when developing and deploying information technology systems containing USPI to ensure effective auditing and reporting as required by these guidelines;
- d. Establish documented procedures for retaining USPI and recording the reason for retaining such information and the authority approving the retention;
- e. Regularly train I&A personnel who access or use USPI on the civil rights, civil liberties, and privacy protections that apply to such information; and
- f. Periodically evaluate the adequacy of the temporary retention periods established for evaluating USPI in Sections 2.2.1 and 3.2.

1.3. REQUIRED CONSULTATION

I&A personnel must consult with the Office of the General Counsel/Intelligence Law Division prior to engaging in any intelligence activity under the following circumstances:

- a. Where the activity contemplated represents a new or significantly revised I&A intelligence initiative;
- b. Where there is any reason to believe that the activity contemplated does not fall within the scope of one or more of the national and departmental missions described above in Section 1.1;
- c. Before tasking a person or organization outside the Intelligence Community or asking such a person or organization to collect intelligence or information on behalf of I&A; or
- d. Before making a request for assistance from another entity pursuant to Section 4.3 below.

2. GUIDELINES FOR COLLECTION, RETENTION, AND DISSEMINATION

This Part establishes the standard guidelines governing the collection, retention, and dissemination of intelligence and information. It does not apply to bulk data transfers, which are subject to the special guidelines set forth in Part Three. At all times, I&A personnel must have a reasonable belief that any intelligence activity they engage in furthers one or more of the national or departmental missions described above in Section 1.1 for the activity to be authorized.

2.1. COLLECTION

I&A personnel may access intelligence or information where they have a reasonable belief that viewing the intelligence or information would further one or more of the national or departmental missions described above in Section 1.1. To proceed from access to collection of the intelligence or information, I&A personnel must also satisfy the requirements and abide by the restrictions described below. There are three categories of these requirements and restrictions: (a) those pertaining to the method of collection (i.e., the requirement that collection be overt or through publicly available sources); (b) those pertaining to collection techniques (e.g., the requirement that collection be made through the least intrusive collection techniques feasible); and (c) those pertaining to the collection of USPI. I&A personnel must satisfy all three categories of requirements and restrictions for collection to be authorized.

2.1.1. Collection Method (Overtly or through Publicly Available Sources)

In accordance with Section 1.7 of Executive Order 12,333, I&A personnel are only authorized to (1) use *overt collection* methods or (2) to collect information from publicly available sources.

2.1.2. Collection Techniques (Least Intrusive Means)

I&A personnel are required to use the least intrusive collection techniques feasible and sufficient when collecting USPI or when collecting intelligence or information within the United States. The collection of such intelligence or information from publicly available sources or with the *consent* of the subject of the intelligence or information is generally less intrusive than collection from a cooperating source. I&A personnel are required to consult with the Office of the General Counsel/Intelligence Law Division prior to taking or refraining from taking any action based upon implied consent to ensure that adequate notice has been provided to the individual consenting to collection.

UNCLASSIFIED

I&A personnel are permitted to engage in *physical surveillance*, the use of *mail covers*, and the use of monitoring devices only to the extent permitted by and consistent with Sections 2.1.2.2–2.1.2.3 below. I&A personnel are not permitted to engage in *electronic surveillance* or unconsented physical searches. Use of these techniques within the United States will be coordinated with the Federal Bureau of Investigation, consistent with Executive Order No. 12,333 or applicable law or memorandum of understanding.

2.1.2.1. *Physical Surveillance*

I&A personnel are permitted to engage in physical surveillance of former or current I&A personnel or applicants to I&A for *counterintelligence* purposes subject to the following requirements:

- a. Any physical surveillance must be approved in writing by the Under Secretary for Intelligence and Analysis (or his or her designee) in consultation with the Office of the General Counsel/Intelligence Law Division;
- b. The surveillance must be performed consistent with standard operating procedures issued by the Under Secretary for Intelligence and Analysis after review by (a) the Office of the General Counsel/Intelligence Law Division to ensure that the procedures are consistent with any applicable legal requirements, (b) the Intelligence Oversight Officer to ensure that the procedures are consistent with these guidelines, and (c) the DHS Privacy Office and DHS Office for Civil Rights and Civil Liberties to ensure that the procedures appropriately protect individuals' privacy, civil rights, and civil liberties. These procedures will identify the standard that the Under Secretary for Intelligence and Analysis will use to approve requests for physical surveillance;
- c. On a DHS facility, any such surveillance must comport with the requirements for overt collection, and such surveillance is prohibited in circumstances where the target of the surveillance has a reasonable expectation of privacy;
- d. While approvals may be renewed, no single approval shall be for a period in excess of 72 hours; and
- e. I&A personnel are not authorized to conduct physical surveillance outside of DHS facilities, but may seek the assistance of a DHS law enforcement component, or an element of the Intelligence Community explicitly authorized to conduct counterintelligence activities pursuant to Executive Order No. 12,333, as

appropriate, to conduct physical surveillance outside of DHS facilities consistent with the assisting organization's authorities.

2.1.2.2. Mail Covers

I&A personnel may request mail covers for mail that is within the possession of the Department of Homeland Security. For all other mail, I&A personnel may seek the assistance of a DHS law enforcement component or the Federal Bureau of Investigation, as appropriate, in requesting that the United States Postal Service perform a mail cover to the extent permitted by and consistent with 39 C.F.R. § 233.3 (2016) (or any succeeding regulation or equivalent authority). Any mail cover must be for counterintelligence purposes and requires the approval of the Office of the General Counsel/Intelligence Law Division. I&A personnel are not otherwise permitted to engage in mail searches.

2.1.2.3. Use of Monitoring Devices

I&A personnel are permitted to use monitoring devices only for counterintelligence purposes and subject to the following requirements and restrictions.

The use of monitoring devices, excluding *concealed monitoring* devices, within the United States or directed at United States Persons is permitted only where (1) the Under Secretary for Intelligence and Analysis (or his or her designee) has determined that the monitoring is necessary to the conduct of an authorized counterintelligence function and (2) the Office of the General Counsel/Intelligence Law Division has determined that the monitoring would occur under conditions where the targets of the monitoring would have no reasonable expectation of privacy, the monitoring does not require trespass, the monitoring does not constitute electronic surveillance, and the monitoring involves either overt collection or the collection of *publicly available information*.

The use of concealed monitoring devices by I&A personnel is not authorized. I&A personnel may seek the assistance of a DHS law enforcement component or the Federal Bureau of Investigation, as appropriate, in requesting the use of concealed monitoring devices consistent with the assisting organization's authorities. Any such request requires the approval of the Office of the General Counsel/Intelligence Law Division.

2.1.3. Collection of USPI

In addition to the requirements and restrictions on collection listed above, I&A personnel are subject to additional requirements and restrictions concerning the collection of USPI. These rules vary for intentional collection of USPI, *incidental collection of USPI*, and USPI that

is volunteered to I&A. Any collection within the United States will be coordinated with the Federal Bureau of Investigation consistent with Executive Order No. 12,333 or applicable law or memorandum of understanding. Any collection outside the United States will be coordinated with the Central Intelligence Agency, as appropriate.

2.1.3.1. Intentional Collection of USPI

I&A personnel may intentionally collect USPI where they have a reasonable belief that the collection activity furthers one or more of the national or departmental missions listed above in Section 1.1 and will result in the acquisition of USPI that falls within one or more of the standard or supplemental information categories described below in Section 2.2.3.

2.1.3.2. Incidental Collection of USPI

I&A personnel may incidentally collect USPI that could not be intentionally collected where the following requirements are satisfied:

- a) Collecting information about the target of the collection is consistent with all applicable requirements of law and policy, including these guidelines;
- b) The incidentally acquired information is not itself deliberately sought; and
- c) It would create an unreasonable burden to collect the information about the target without collecting the additional, non-targeted information.

2.1.3.3. Volunteered USPI

I&A personnel may collect volunteered USPI that could not be intentionally or incidentally collected where (a) the USPI is not received through the action or at the behest of I&A personnel and (b) there is no mutual expectation between I&A and the provider of the USPI, whether explicit or inferred based upon past practice, that such information is to be provided on a regular or recurring basis.

2.2. RETENTION

The retention of intelligence or information, whether collected or otherwise obtained by I&A, is permitted only to the extent there is a reasonable belief that retention furthers one or more of the national or departmental missions listed above in Section 1.1 and the USPI falls within one of two categories: (a) retention for evaluation or (b) permanent retention. Retention in either of these categories is subject to requirements and restrictions, as set forth below.

2.2.1. Retention for Evaluation

As an initial matter, I&A personnel may temporarily retain USPI for the limited purpose of evaluating whether the USPI qualifies for permanent retention by I&A. The evaluation period cannot exceed 180 days from the date on which the USPI is collected unless the USPI is not initially believed to be USPI, in which case the evaluation period commences from the date on which the USPI is known or reasonably should have been known to constitute USPI. I&A personnel must delete all USPI that does not qualify for permanent retention pursuant to Section 2.2.2 below once the evaluation period expires or when it is conclusively determined that the USPI does not qualify for permanent retention by I&A, whichever occurs first. This section does not apply to bulk data transfers, which are subject to the special guidelines set forth in Part Three.

These requirements notwithstanding, I&A personnel may temporarily retain USPI for further evaluation for additional 180-day increments—but in any event no longer than five years total—where (a) the Under Secretary for Intelligence and Analysis determines that there is a significant likelihood based upon the content of the USPI and/or the circumstances under which it was encountered that further evaluation will result in the identification of intelligence or information that qualifies for permanent retention pursuant to Section 2.2.2 below, (b) the Office of the General Counsel/Intelligence Law Division is afforded an opportunity to consider in a timely manner whether further retention would violate any applicable legal requirements, (c) the Intelligence Oversight Officer is afforded an opportunity to consider in a timely manner whether further retention would be consistent with these guidelines, and (d) the DHS Privacy Office and the DHS Office for Civil Rights and Civil Liberties are afforded an opportunity to consider in a timely manner whether the technical and policy safeguards under which the USPI would be retained are sufficient to appropriately protect the privacy, civil rights, and civil liberties of the United States Persons whose information is subject to evaluation.

2.2.2. Permanent Retention

I&A personnel may permanently retain USPI where the USPI furthers one or more of the national or departmental missions listed above in Section 1.1 and falls within one or more of the standard or supplemental information categories set forth in Section 2.2.3. I&A personnel must record or denote the authorized national or departmental mission or missions (of those listed above in Section 1.1) that would be furthered by permanent retention and the standard or supplemental information category or categories of information (of those listed in Section 2.2.3) that permit the permanent retention of the USPI. Further, I&A personnel must identify and mark files reasonably believed to contain

USPI and, to the greatest extent possible, mark specific files and documents containing USPI in accordance with standards promulgated by the Director of National Intelligence regardless of the format or location of the USPI or the method for storing such USPI. Where I&A personnel conclude that permanently retained USPI no longer satisfies the requirements for permanent retention set forth above, they will delete all forms of that USPI regardless of format or location.

2.2.3. Information Categories

Standard information categories support I&A's national missions under Section 1.1.1, while supplemental information categories support I&A's departmental missions under Section 1.1.2; like I&A's missions, these standard and supplemental information categories are not exclusive of one another.

I&A personnel may collect and retain USPI that falls within one or more of the following standard or supplemental information categories so long as that collection or retention comports with all other applicable provisions of these Guidelines.

2.2.3.1. Standard Information Categories

- a. Consent: The USPI of a United States Person who has consented to collection of the information.
- b. Publicly Available: The USPI is publicly available.
- c. Foreign Intelligence: The USPI is reasonably believed to constitute *foreign intelligence* where the USPI falls within one or more of the subcategories listed below.
 - i. Foreign Intelligence (International Terrorism): The USPI is reasonably believed to relate to the existence, organization, capabilities, plans, intentions, means of finance or material support, or activities of groups or individuals involved in international terrorism; to threats posed by such groups or individuals to the United States, United States Persons, or United States interests, or to those of other nations; or to communications between such groups and other individuals reasonably believed to be assisting or associating with them to such a degree that collection of USPI concerning such associates would assist in understanding international terrorism.

UNCLASSIFIED

- ii. Foreign Intelligence (International Narcotics Activities): The USPI is reasonably believed to relate to activities outside the United States involving the production, transfer, or distribution of significant quantities of narcotics or other controlled substances in violation of Federal law, or activities within the United States that are directly connected to such activities.

- iii. Foreign Intelligence (Other): The USPI is reasonably believed to constitute foreign intelligence even if that foreign intelligence does not pertain to international terrorism or international narcotics activities as described above under the following circumstances:
 - 1. Where the USPI concerns an individual reasonably believed to be an officer or employee, or otherwise acting for or on behalf of, a foreign power;
 - 2. Where the USPI concerns an organization or group reasonably believed to be owned or controlled, directly or indirectly, by a foreign power;
 - 3. Where the USPI concerns a corporation or other commercial organization reasonably believed to be acting for or on behalf of a foreign power, organization, or person engaged in clandestine intelligence activities, sabotage, assassinations, or international terrorist activities;
 - 4. Where the USPI concerns an individual, organization, or group reasonably believed to be engaged in or preparing for—on behalf of a foreign power—attacks on or intrusions into DHS information systems, any DHS contractors' information systems that impact DHS personnel, property, or missions, or Federal Government national security systems; or
 - 5. Where the USPI concerns an individual reasonably believed to be a prisoner of war, missing in action, or (other than with respect to members of the Armed Forces) engaged or involved in an armed conflict or hostilities abroad, or who is the target, hostage, or victim of an international terrorist organization.

- d. Counterintelligence: The USPI is reasonably believed to relate to an individual, organization, or group reasonably believed to be engaged in or preparing for

UNCLASSIFIED

espionage, other intelligence activities, sabotage, or assassination on behalf of a foreign power, organization, or person, or the USPI is reasonably believed to relate to a United States Person in contact with such an individual, organization, or group, but only for the purpose of identifying that United States Person and assessing any relationship between the United States Person and such individual, organization, or group.

- e. Investigative Information: The USPI is reasonably believed to have been acquired in the course of a lawful foreign intelligence, counterintelligence, international drug trafficking, or international terrorism investigation.
- f. Threats to Safety: The USPI is reasonably believed to be necessary to protect against a clear, imminent threat to the safety of any person or organization, including those who are targets, victims, or hostages of international terrorist organizations.
- g. Protection of Intelligence Sources and Methods: The USPI is reasonably believed to concern individuals who have access to, had access to, or are otherwise in possession of information that reveals foreign intelligence or counterintelligence sources or methods or activities, provided that such USPI is reasonably believed to be necessary to protect against the unauthorized disclosure of such information, and provided that, within the United States, I&A personnel are required to limit the collection of USPI to persons who are (i) present or former employees of I&A, (ii) present or former contractors of I&A or their present or former employees, or (iii) applicants for such employment or contracting.
- h. Current, Former, or Potential Sources of Assistance: The USPI is reasonably believed to concern individuals who are or have been sources of information or assistance or who are reasonably likely to be of value as sources of information or assistance to the intelligence activities of I&A (or any other element of the Intelligence Community for whom the source would be useful) for the purpose of assessing their suitability or credibility, except that this category does not include USPI arising in investigations undertaken for personnel security purposes. Any such collection requires approval by the Under Secretary for Intelligence and Analysis accompanied by notice to the Intelligence Oversight Officer and the Associate General Counsel for Intelligence.

UNCLASSIFIED

- i. Personnel, Physical, and Communications Security: The USPI is reasonably believed to have been obtained pursuant to a lawful personnel, physical, or communications security investigation.
- j. Overhead Reconnaissance: The USPI is reasonably believed to have been collected by overhead reconnaissance that was not directed at specific United States Persons.

2.2.3.2. Supplemental Information Categories

- a. Critical Infrastructure and Key Resources: The USPI is reasonably believed to relate to threats to or the vulnerabilities of the critical infrastructure or key resources of the United States, including, but not limited to, cyber security threats or weapons of mass destruction.
- b. Border Security: The USPI is reasonably believed to relate to threats to the safety or integrity of the United States borders, including, but not limited to, information about individuals engaging in activities that violate or are intended to violate immigration or customs laws or regulations.
- c. Domestic Terrorism: The USPI is reasonably believed to relate to the existence, organization, capabilities, plans, intentions, means of finance or material support, or activities of domestic groups or individuals involved in domestic terrorism; to threats posed by such groups or individuals to the United States, United States Persons, or United States interests; or to communications between such groups or individuals reasonably believed to be assisting or associating with them to such a degree that retention of USPI concerning such associates would assist in understanding domestic terrorist groups or individuals involved in domestic terrorism.
- d. Vulnerabilities: The USPI is reasonably believed to relate to vulnerabilities to international or domestic terrorism or other threats to homeland security.
- e. Departmental Investigative Information: The USPI is reasonably believed to have been acquired in or relevant to the course of a lawful departmental investigation or enforcement action.

- f. Major Disasters: The USPI is reasonably believed to be necessary to understand, prevent, preempt, deter, or respond to major natural or manmade disasters or other catastrophic acts.
- g. Protected Individuals, Groups, and Events: The USPI is reasonably believed to relate to threats to individuals, groups, property, or events protected by the Department of Homeland Security, including Components within the Department.
- h. Other Threats to Homeland Security: The USPI is reasonably believed to relate to any other threat of such severity and magnitude that Federal assistance is needed to supplement State and local efforts or capabilities to save lives and to protect property and public health and safety, or to lessen or avert the threat of a catastrophe in any part of the United States, including, but not limited to, significant threats to the Nation's economic security, public health, or public safety.

2.2.4. Additional Requirements for Certain Communications

In addition to complying with the requirements for evaluation or permanent retention as described above in Sections 2.2.1–2.2.2, I&A personnel may retain telephonic or electronic communications subject to Section 309 of the Intelligence Authorization Act for Fiscal Year 2015 for more than five years only where they comply with the requirements of Section 309(b)(3)(B) of that Act.

2.3. DISSEMINATION

Like collection and retention, the dissemination of intelligence or information is permitted only to the extent there is a reasonable belief that dissemination furthers one or more of the national or departmental missions listed above in Section 1.1. The dissemination of USPI is subject to additional requirements and restrictions. These requirements and restrictions vary according to whether the dissemination is to another element of the Intelligence Community or outside the Intelligence Community.

2.3.1. General Dissemination Requirements

I&A personnel may disseminate USPI where all three of the following requirements are met:

- a. The USPI is permanently retainable by I&A pursuant to Section 2.2.2 above;

- b. The recipient is one of the following:
- i. A Federal, State, local, tribal, or territorial government entity (not including an element of the Intelligence Community) with law enforcement, counterterrorism, or national or homeland security-related functions;
 - ii. An element of the Intelligence Community, and the USPI relates to a standard information category identified in Section 2.2.3.1 above, or, where the USPI relates only to a supplemental information category identified in Section 2.2.3.2 above, I&A personnel have confirmed the recipient's authority to receive the USPI;
 - iii. A foreign government, international, or multinational entity;
 - iv. Another element or office of the Department; or
 - v. A private sector entity or individual with responsibilities relating to homeland security; and
- c. There is a reasonable belief that dissemination would assist the recipient of the USPI in fulfilling one or more of the recipient's lawful intelligence, counterterrorism, law enforcement, or other homeland security-related functions.

2.3.2. Dissemination of Unevaluated Information within the Intelligence Community

Notwithstanding the general dissemination requirements of Section 2.3.1 above, and in accordance with E.O. 12,333 Section 2.3, I&A personnel may disseminate USPI to other appropriate elements of the Intelligence Community for purposes of allowing the recipient Intelligence Community element to determine whether the information is relevant to its responsibilities and can be retained by it. This dissemination is permitted both where the USPI is being temporarily retained by I&A for evaluation to determine whether it may be permanently retained by I&A in accordance with Sections 2.2.2 and 2.2.3.1 above (in which case neither the 180 day cap on evaluation nor the conclusive determination *deletion* requirement of Section 2.2.1 will apply to other elements of the Intelligence Community), or where the I&A personnel choose to disseminate the unevaluated USPI in accordance with the bulk data procedures set forth in Section 3.3 below.

2.3.3. Dissemination with Approval

The requirements set forth above in Sections 2.3.1–2.3.2 notwithstanding, I&A personnel may disseminate USPI outside I&A where such dissemination is approved by the Under Secretary for Intelligence and Analysis in consultation with the Associate General Counsel for Intelligence, the Chief Privacy Officer, the Officer for Civil Rights and Civil Liberties, the Intelligence Oversight Officer, and the Assistant Attorney General for National Security. Approval will only be granted where dissemination is permitted by and consistent with applicable law and policy and is done in a manner that appropriately protects the privacy, civil rights, and civil liberties of the United States Persons whose information would be disseminated.

2.3.4. Additional Requirements for Foreign Disseminations

In addition to the general requirements for dissemination described above, the dissemination of USPI to foreign governments or international or multinational entities is permissible only where the Under Secretary for Intelligence and Analysis or his or her designee determines that dissemination (disclosure or release) of the USPI is consistent with any applicable international agreements and foreign disclosure and release policies and directives, including any policies and directives requiring analysis of harm to any individual.

2.3.5. Anonymization Requirement

Prior to disseminating USPI pursuant to either Section 2.3.1 or Section 2.3.3, I&A personnel must evaluate whether the USPI would materially assist the intended recipient in using or understanding the disseminated intelligence or information. Where including the USPI would not materially assist the intended recipient in this manner, I&A personnel must replace it with a generic marking identifying the individual as a United States Person (e.g., “U.S. Person,” “USPER,” etc.). Where USPI is included, notice of that information must be provided through an advisory indicating that USPI is contained within the record or document being disseminated and by highlighting the USPI in a manner that clearly identifies it as such. These requirements do not apply to the dissemination of (1) publicly available information; (2) USPI disseminated with the consent of the person concerned; or (3) intelligence products or reports originating from other Intelligence Community elements provided those products or reports are not materially authored or altered by I&A personnel.

3. SPECIAL GUIDELINES FOR BULK DATA TRANSFERS

This Part establishes special guidelines applicable to bulk data transfers reasonably likely to contain USPI. It applies only to bulk data transfers to or from I&A and is an alternative to

UNCLASSIFIED

the collection, retention, or dissemination standard procedures set forth above. Except as otherwise specified, bulk data transfers conducted under this Part are not subject to collection, retention, and dissemination requirements described in Part 2. This Part does not apply to bulk data transfers that are not reasonably likely to contain USPI, or to bulk data transfers (or segregable portions of bulk data transfers) that can be permanently retained by I&A upon receipt consistent with Section 2.2.2 above. Except as provided in the last paragraph of Section 3.2 below, these requirements also do not apply to *bulk data collection* of volunteered information. I&A may engage in the bulk data collection of volunteered information subject to the same standard requirements and restrictions governing the collection of volunteered information as set forth above at Section 2.1.3.3. Finally, the guidelines do not apply to bulk data transfers consisting exclusively of publicly available information, information whose use or dissemination is governed by court order or other procedures approved by the Attorney General, or information contained in intelligence products or reports obtained by I&A personnel in the ordinary course of their official duties. Where USPI in a bulk data transfer is identified and segregated from the remainder of the information, the requirements and restrictions provided below apply only to the USPI, not the remainder of the information.

As with all of its intelligence activities, I&A is authorized to engage in bulk data transfers only where it is reasonable to believe that a transfer to or from I&A would further one or more of the national or departmental missions listed above in Section 1.1, and all bulk data collection must be overt or through publicly available sources consistent with the requirements of Section 2.1.1 above. Further, any bulk data transfers to or from I&A must be permitted by and consistent with any applicable departmental policies or procedures. Generally, the Department encourages the use of alternatives to bulk data transfers, such as the provision of account access, the provision of specific records in response to requests for information, or the comparison of data within DHS-controlled environments, where those alternatives adequately support the information needs of the requestor. Accordingly, all bulk data transfers reasonably likely to contain USPI must be approved by the Under Secretary for Intelligence and Analysis after providing an opportunity for timely consideration by (a) the Office of the General Counsel to ensure that any such transfers are consistent with any applicable legal requirements, (b) the Intelligence Oversight Officer to ensure that any such transfers are consistent with these guidelines, and (c) the DHS Privacy Office and DHS Office for Civil Rights and Civil Liberties to ensure that any such transfers are conducted in a manner that appropriately protects individuals' privacy, civil rights, and civil liberties. The Under Secretary for Intelligence and Analysis, working with the Office of the General Counsel/Intelligence Law Division, the DHS Privacy Office, the DHS Office for Civil Rights and Civil Liberties, and the Intelligence Oversight Officer, will review I&A bulk data

collections not previously determined to contain USPI every three years to assess whether this determination remains accurate.

3.1. BULK DATA COLLECTION

With the exception of volunteered information, I&A may engage in a bulk data collection containing USPI only where two requirements are met. First, prior to engaging in the bulk data collection, the Under Secretary for Intelligence and Analysis must make the following determinations in writing:

- a. A determination that bulk data collection is the only practicable means of identifying or using the information in the collection that will support an authorized I&A mission (of the list set forth above in Section 1.1);
- b. A determination that, to the greatest extent practicable, only those data elements that are reasonably likely to support an authorized I&A mission (of the list set forth above in Section 1.1) are collected; and
- c. A determination that the bulk data collection is reasonable in light of the totality of the circumstances, including, but not limited to, the following:
 - i. The expected contribution of the bulk data collection to a national or departmental mission;
 - ii. The methods and means by which the information was acquired and/or aggregated by the data provider;
 - iii. The volume, proportion, nature, and sensitivity of the personally identifiable information collected; and
 - iv. The safeguards to be applied to the collected information.

Second, any bulk data collection containing USPI will be subject to terms and conditions issued by the Under Secretary for Intelligence and Analysis. Prior to issuance, these terms and conditions will be submitted for timely consideration by (a) the Office of the General Counsel to ensure that the terms and conditions are consistent with any applicable legal requirements, (b) the Intelligence Oversight Officer to ensure that the terms and conditions are consistent with these guidelines, and (c) the DHS Privacy Office and DHS Office for Civil Rights and Civil Liberties to ensure that the terms and conditions appropriately

UNCLASSIFIED

protects individuals' privacy, civil rights, and civil liberties. These terms and conditions must include the following protections for USPI:

- a. A requirement that any I&A personnel provided access to the bulk data collection receive training in the use of that information to ensure they understand the safeguards applicable to the information and any other requirements involved in accessing and using the information;
- b. A requirement that the bulk data collection be received, stored, and used in a secure manner that appropriately protects intelligence sources and methods and related sensitivities consistent with all applicable legal and policy requirements;
- c. A defined period of time during which the bulk data collection will be retained for evaluation pursuant to Section 3.2 below; and
- d. A description of the means and methods by which the bulk data collection will be evaluated.

These terms and conditions must also include any other safeguards for USPI that are appropriate under the circumstances. Examples include the following:

- a. Procedures for the review, approval, or enhanced auditing of any access to or searches conducted in the bulk data collection;
- b. Procedures to restrict access to or dissemination from the bulk data collection;
- c. Procedures to mask any personally identifiable information within the bulk data collection;
- d. Physical or logical access controls for the bulk data collection, including data segregation or policy-, attribute-, or role-based access;
- e. A requirement that I&A use reasonable measures to identify and mark USPI within the data transferred in bulk to the extent appropriate;
- f. Reporting metrics on the use and disposition of personally identifiable information within the bulk data collection to the extent appropriate;

- g. Appropriate procedures to address the correction of any erroneous or outdated data and, where appropriate, individual redress;
- h. Appropriate conditions on third-party dissemination;
- i. Regular reporting, or reviews by the Office of the General Counsel/Intelligence Law Division, the DHS Privacy Office, the DHS Office for Civil Rights and Civil Liberties, and the Intelligence Oversight Officer regarding the use of the bulk data, including the application of any advanced analytic tools to the data, any sharing of the data with third parties, and whether there continues to be a need for retention of the data in bulk; and
- j. Limitations on the amount of time personally identifiable information within the bulk data collection is subject to access and use by I&A personnel.

These terms and conditions may be memorialized in an agreement with the data provider or internally by I&A. If the terms and conditions are developed internally, I&A must make reasonable efforts to provide the data provider with notice of the internal terms and conditions. Generally, they should be developed and executed prior to collection, but they must be developed and executed before the data collected is made available for any analytic or other intelligence uses.

3.2. RETENTION OF BULK DATA COLLECTIONS

I&A retains bulk data collections, including any USPI within the collections, for the limited purpose of evaluating whether records within the collections constituting or containing USPI qualify for permanent I&A retention under the standard requirements and restrictions applicable to permanent retentions as set forth in Section 2.2.2 above. This evaluation must be performed within a defined evaluation period, which commences when the bulk data collection is first made available for evaluation following any necessary formatting, testing, and loading. Records that are determined to neither constitute nor contain USPI and records constituting or containing USPI that qualify for permanent retention pursuant to Section 2.2.2 above may be retained beyond the evaluation period. All other records, including, but not limited to, paper and electronic copies, must be deleted once the evaluation period expires.

The evaluation period for each bulk data collection is memorialized in the terms and conditions governing that bulk data collection as required by Section 3.1 above. As an initial matter, the evaluation period may not exceed five years. I&A may, however, extend the

evaluation period in one-year increments where (a) the Under Secretary for Intelligence and Analysis determines that there is a significant likelihood that further evaluation of the bulk data collection will identify intelligence or information that that qualifies for permanent retention pursuant to Section 2.2.2 above, (b) the Office of the General Counsel/Intelligence Law Division concludes in a timely manner that further retention would not violate any applicable legal requirements, (c) the Intelligence Oversight Officer concludes in a timely manner that further retention would be consistent with these guidelines, and (d) the DHS Privacy Office and the DHS Office for Civil Rights and Civil Liberties conclude in a timely manner that that the technical and policy safeguards under which the USPI would be retained are sufficient to appropriately protect the privacy, civil rights, and civil liberties of the United States Persons whose information is subject to evaluation. The maximum evaluation period for a bulk data collection, including any extensions granted by the Under Secretary for Intelligence and Analysis, is ten years.

Bulk data collections that are volunteered to I&A or collected without preexisting terms and conditions are subject to the standard requirements and restrictions governing retention for evaluation as set forth above at Section 2.2.1 unless I&A executes terms and conditions as described above in Section 3.1. Further, any retention of telephonic or electronic communications subject to Section 309 of the Intelligence Authorization Act of 2015 will be retained for no more than five years unless further retention satisfies the requirements of Section 309(b)(3)(B) of that Act.

3.3. BULK DATA DISSEMINATIONS

I&A may engage in a *bulk data dissemination* of unevaluated information reasonably likely to contain USPI to another element of the Intelligence Community in one of two ways, as directed by the Undersecretary for Intelligence and Analysis or his designee following consideration by (a) the Office of the General Counsel/Intelligence Law Division to ensure that the protections are consistent with any applicable legal requirements, (b) the Intelligence Oversight Officer to ensure that the protections are consistent with these guidelines, and (c) the DHS Privacy Office and DHS Office for Civil Rights and Civil Liberties to ensure that the protections appropriately safeguard individuals' privacy, civil rights, and civil liberties. Under the first, the recipient agrees to provide protections to the data that are comparable to those provided by I&A. For example, the recipient Intelligence Community element's application of its own Attorney General-approved procedures to the bulk data may constitute comparable protection. Under the second, I&A will negotiate alternative protections, memorialized in written terms and conditions between the recipient element head (or his or her designee) and the Under Secretary for Intelligence and Analysis.

I&A may only engage in a bulk data dissemination reasonably likely to contain USPI to an entity outside the Intelligence Community pursuant to written terms and conditions established between the Under Secretary for Intelligence and Analysis and an authorized representative of the recipient of the dissemination. All bulk data disseminations to foreign governments or international or multinational entities are subject to the requirements and restrictions set forth above in Section 2.3.4.

The Under Secretary for Intelligence and Analysis must consult with the Office of the General Counsel/Intelligence Law Division, the Privacy Office, the Office for Civil Rights and Civil Liberties, and the Intelligence Oversight Officer before agreeing to terms and conditions with either an Intelligence Community element or an external entity. Moreover, the terms and conditions must include the protections required in the second paragraph of Section 3.1. Generally, they must be developed and executed prior to dissemination. I&A may, however, engage in bulk data dissemination where the Under Secretary for Intelligence and Analysis determines that there are exigent circumstances (as described below in Section 5.3) requiring the dissemination. Where an emergency dissemination of that nature occurs, the terms and conditions governing the bulk data dissemination will be established as soon as possible, but in any event before any further bulk data dissemination unrelated to the exigent circumstances occurs.

4. GUIDELINES FOR OTHER ACTIVITIES

This Part establishes guidelines for the conduct of certain other activities by I&A personnel as described below.

4.1. PARTICIPATION IN ORGANIZATIONS WITHIN THE UNITED STATES

I&A personnel may only participate in organizations within the United States or organizations outside the United States that are United States Persons to the extent permitted by and consistent with the requirements set forth below.

4.1.1. Conduct Rising to the Level of Participation

I&A personnel participate in an organization when they take part in an organization's activities and interact with its members within the structure or framework of the organization. Such actions include, but are not limited to, the following:

- a. Joining or acquiring membership;

UNCLASSIFIED

- b. Attending or taking part in organizational meetings, academic activities, seminars, trade fairs, workshops, conferences, exhibitions, symposia, social functions, or fora for communication through the use of technology;
- c. Carrying out the work or functions of the organization;
- d. Serving as a representative of the organization; or
- e. Contributing funds to the organization other than in payment for goods or services.

Participation does not include occasional passive attendance at events that are open to the public, including non-members; however, it does include attending or taking part in any meetings or activities—even passively—of an organization that is closed to the public (i.e., meetings or activities exclusive to members and/or invited guests). Participation also does not include taking part in events outside the organizational structure or framework of an organization, such as infrequent attendance at meetings or occasional social gatherings that involve the organization’s members, but that are not functions or activities conducted on behalf of the organization itself.

4.1.2. Participation on Behalf of I&A

Subject to the exceptions set forth below, I&A personnel are authorized to participate in an organization in the United States or organization outside the United States that is a United States Person on behalf of I&A only where two requirements are met. First, I&A personnel or personnel from another Intelligence Community element—not necessarily the actual participant—must disclose to an executive officer of the organization or an official in charge of membership, attendance, or the records of the organization that the participant is affiliated with I&A. If the disclosure is made to an official who is also acting on behalf of I&A, the disclosure requirement is not satisfied unless that official is the most senior official within the organization.

Second, the participation must be approved by the Under Secretary for Intelligence and Analysis in consultation with the Associate General Counsel for Intelligence. The approval by the Under Secretary for Intelligence and Analysis is valid for the duration of the participation or twelve months, whichever is shorter. Re-approval is required for any further participation.

These requirements do not apply under the following circumstances:

UNCLASSIFIED

- a. Where the employee or contractor is participating in, but not eliciting information from, a group on a social media or Internet platform, provided that the group's activities are publicly available;
- b. Where the employee or contractor is attending a commercial class or training on behalf of I&A, provided that the employee or contractor is not tasked or directed to collect intelligence and the true name and I&A affiliation of the employee or contractor is used;
- c. Where the employee or contractor is only obtaining the publication of an organization whose membership is open to the general public;
- d. Where the employee or contractor is participating in an educational or professional organization to enhance the employee's or contractor's professional skills, knowledge, or capabilities;
- e. Where the employee or contractor is participating in an organization that is an official establishment of a foreign government; or
- f. Where the employee or contractor is participating in a seminar, forum, conference, exhibition, trade fair, workshop, symposium, or similar meeting, whether in person or through social media, provided that (i) the meeting is sponsored by an organization in which the employee or contractor is a member or for which the employee or contractor has been invited to participate; and (ii) the purpose of participation is to collect significant foreign intelligence that is generally made available to participants at such meetings and does not involve the domestic activities of the organization or its members.

In addition to the notice and approval requirements described above, I&A personnel may participate in social media platforms on behalf of I&A only to the extent permitted by and consistent with applicable departmental and I&A policies and guidelines. I&A personnel are prohibited from participating in an organization on behalf of I&A for the purpose of influencing the activities of an organization or its members except where (a) the participation is undertaken on behalf of the Federal Bureau of Investigation in the course of a lawful investigation or (b) the organization is composed primarily of individuals who are not United States Persons and is reasonably believed to be acting on behalf of a foreign power. Finally, I&A personnel participating in an organization on behalf of I&A are permitted to collect intelligence or information for intelligence purposes only to the extent permitted by and

consistent with Section 2.1 above, including, but not limited to, the requirement that any such collection be conducted overtly or through publicly available sources.

4.1.3. Participation in a Personal Capacity

The requirements and restrictions described above in Section 4.1.2 apply to I&A personnel participating in an organization on behalf of I&A. I&A personnel are permitted to participate in organizations in a personal capacity (i.e., on their own initiative and expense solely for personal benefit) without restriction provided that they do not, in their official capacities, collect, retain, or disseminate any intelligence or information provided or maintained by the organization or its members. This rule against the use of personal membership for an official purpose in no way restricts I&A personnel who are participating in an organization in an exclusively personal capacity from reporting actual or suspected violations of law, threats to national or homeland security, or foreign intelligence or counterintelligence to appropriate Federal, State, and local law enforcement, homeland security, or intelligence authorities in their personal capacities.

4.2. ASSISTANCE TO LAW ENFORCEMENT AND OTHER CIVIL AUTHORITIES

In addition to accessing intelligence and information held by, collecting intelligence and information from, and disseminating intelligence and information to law enforcement and other civil authorities as described in Part Two of these guidelines, I&A personnel are authorized to assist law enforcement and other civil authorities as follows:

- a. By cooperating with appropriate law enforcement agencies for the purpose of protecting the employees, information, property, and facilities of any element of the Intelligence Community;
- b. Unless otherwise precluded by law or Executive Order No. 12,333, “United States Intelligence Activities,” as amended July 30, 2008, by participating in law enforcement activities to investigate or prevent clandestine intelligence activities by foreign powers, or to investigate or prevent international terrorist or international narcotics activities, provided that such participation is approved in each case by the Office of the General Counsel/Intelligence Law Division;
- c. By providing specialized equipment, technical knowledge, or assistance of expert personnel for use by any Federal department or agency or, when lives are endangered, to support State, local, tribal, or territorial law enforcement agencies

provided that such assistance is approved in each case by the Office of the General Counsel/Intelligence Law Division; or

- d. As otherwise required or authorized by law.

4.3. REQUESTS FOR ASSISTANCE

I&A personnel are authorized to request assistance in the accessing, collection, retention, analysis, production, or dissemination of intelligence or information, including USPI, and including through the use of techniques or methods not authorized for I&A personnel, by any entity where they have a reasonable belief that the assistance requested would support one or more of the national or departmental missions listed above in Section 1.1 and the assistance requested is permitted by and consistent with applicable law and policy governing the activities of the recipient of the request, including, to the extent applicable, the recipient's own intelligence oversight guidelines approved by the Attorney General. I&A personnel must consult with the Office of the General Counsel/Intelligence Law Division prior to making a request for assistance pursuant to this section.

4.4. SHARED REPOSITORIES

Neither I&A's hosting another entity's intelligence or information in a *shared repository*, nor providing system administrative or technical support functions to a shared repository constitute the collection, retention, or dissemination by I&A of the intelligence or information held in that repository. As a result, these guidelines do not apply to I&A personnel who are engaging solely in such activities. Each participant in a shared repository hosted by I&A must inform I&A that its participation complies with all applicable law, policies, and procedures. To the extent practicable, I&A should enable audit of access to USPI in any shared repository that it hosts.

If I&A personnel participate in a shared repository, including a shared repository hosted by I&A, for operational or analytic intelligence purposes (i.e., for purposes beyond those described above), then their participation must be in accordance with these guidelines and in accordance with any more restrictive rules required by the host of the shared repository. With respect to information or intelligence provided by I&A, however, I&A may allow the host or another Intelligence Community element to provide system administrative or technical support functions without complying with the requirements of Parts Two and Three.

5. MISCELLANEOUS PROVISIONS

This Part sets forth the administrative and other miscellaneous provisions facilitating the execution and implementation of these guidelines.

5.1. EFFECTIVE DATE

These guidelines are effective as of the date of approval by the Secretary of Homeland Security and the Attorney General.

5.2. INTERPRETATION

Questions regarding the interpretation of these guidelines should be referred to the Office of the General Counsel/Intelligence Law Division. Questions regarding the execution or implementation of the guidelines should be referred to the Intelligence Oversight Officer. The Under Secretary for Intelligence and Analysis, acting through the Office of the General Counsel/Intelligence Law Division, will consult with the Department of Justice's National Security Division and the Office of the Director of National Intelligence's Office of the General Counsel regarding novel or significant interpretations of these guidelines, as appropriate.

5.3. DEPARTURES

Subject to the exception for exigent circumstances listed below, departures from these guidelines are permitted only where and to the extent authorized in advance by both the Under Secretary for Intelligence and Analysis and the Assistant Attorney General for National Security after consultation with the Director of National Intelligence. Notice of any departures must be provided to the Associate General Counsel for Intelligence and to the Intelligence Oversight Officer for referral to the DHS Chief Privacy Officer where the departure implicates individuals' privacy and/or DHS Officer for Civil Rights and Civil Liberties where the departure implicates individuals' civil rights or civil liberties. Any activities constituting a departure from these guidelines must be carried out in accordance with the Constitution and the laws of the United States under all circumstances.

The requirement for authorization from the Assistant Attorney General for National Security set forth above does not apply to departures from these guidelines in exigent circumstances where the Under Secretary for Intelligence and Analysis or a delegate determines that, due to the immediacy or gravity of a threat to the safety of persons or property or to the national security, such authorization cannot be obtained in advance (i.e., a clear, imminent threat of such severity exists that the failure to depart from the provisions of

these guidelines would be reasonably likely to endanger the safety of persons or property or the national or homeland security and the departure contemplated would be reasonably likely to prevent, preempt, deter, or respond to the threat). Any departures from these guidelines pursuant to this exception must be reported to the Associate General Counsel for Intelligence for further referral to the Assistant Attorney General for National Security and Director of National Intelligence and the Intelligence Oversight Officer for further referral to the DHS Chief Privacy Officer where the departure implicates individuals' privacy and/or the DHS Officer for Civil Rights and Civil Liberties where the departure implicates individuals' civil rights or civil liberties. This notice must be provided as soon as is practicable, but in any event no later than three working days from the authorization for departure.

5.4. AMENDMENTS

Subject to the exception for supplemental information categories listed below, amendments to these guidelines are permitted only where and to the extent authorized in advance by both the Secretary of Homeland Security and the Attorney General, after consulting with the Director of National Intelligence.

The Under Secretary for Intelligence and Analysis is authorized to add other supplemental information categories to the list provided above in Section 2.2.3.2 subject to the following requirements and restrictions. First, to add a supplemental information category, the Under Secretary for Intelligence and Analysis must determine that the proposed category is narrowly tailored to support an authorized departmental mission as described above in Section 1.1. This determination is subject to review for legal sufficiency by the General Counsel, who must certify that the proposed category is legally sufficient for the proposed category to be added.

Second, the Under Secretary for Intelligence and Analysis must provide notice to the Assistant Attorney General for National Security and the Director of National Intelligence of his or her intent to add a supplemental information category to the list provided above in Section 2.2.3.2. Notice must be provided as soon as is practicable, but in any event no later than thirty days prior to addition of the category. If the Assistant Attorney General for National Security or the Director of National Intelligence object to the addition of the proposed category within thirty days of receipt of notice from the Under Secretary for Intelligence and Analysis that he or she intends to add the proposed category, the proposed category will not be added unless and until the objecting party and the Under Secretary for Intelligence and Analysis resolve the objection. If the Assistant Attorney General for National Security and the Director of National Intelligence affirmatively indicate their

approval of the proposed category or fail to object to the category within thirty days of receipt of notice from the Under Secretary for Intelligence and Analysis, the category will be added to the list provided above. Any supplemental information category added pursuant to this section must be memorialized via amendment to these guidelines, with notice of the additional category provided to the Associate General Counsel for Intelligence, the Chief Privacy Officer, the Officer for Civil Rights and Civil Liberties, and the Intelligence Oversight Officer.

5.5. DELEGATION

Where these guidelines require a specific official to approve an activity or take some other action, only that official or a more senior official is permitted to take that action.

GLOSSARY OF DEFINED TERMS

- A. **Access**: The act of viewing or examining information or intelligence without collecting that information or intelligence.
- B. **Bulk Data Collection**: Collection via bulk data transfer.
- C. **Bulk Data Dissemination**: Dissemination via bulk data transfer.
- D. **Bulk Data Transfer**: The transfer of large quantities of data that, due to technical or operational considerations, is acquired without the use of discriminants (e.g., specific identifiers, selection terms, etc.). As a matter of DHS policy, bulk data transfer also includes the collection or dissemination of large quantities of data, a significant portion of which is not reasonably likely to have any ultimate intelligence or operational value to the recipient, but which is provided for the recipient to identify information of intelligence or operational value within it. Bulk data transfer does not include the transfer of records responsive to specific identifiers (e.g., name, date of birth, social security number, etc.) but it does include the transfer of records identified through the application of search terms where the transfer would include a significant number of records that, while responsive to the applied search terms, is not reasonably likely to have any ultimate intelligence or operational value to the recipient (e.g., records responsive to demographic profiles such as age, citizenship, or gender).
- E. **Collection**: Obtaining or acquiring information from outside the Intelligence Community (including from the Office of the Secretary and other Components) by any means, including, but not limited to, information that is volunteered, and regardless of whether the information is temporarily or permanently retained. Information that only momentarily passes through an I&A computer system is not collected. Collection is distinct from access to information in that collection requires that the information be copied, saved, or used in some manner, including, but not limited to, information that is copied or saved in the form of summaries, reports, or notes, whereas information that is accessed is merely viewed or examined, but is not collected even if it is transmitted on an I&A information technology system.
- F. **Concealed Monitoring**: The use of hidden electronic, optical, or mechanical devices to monitor a particular person or a group of persons without their consent in a surreptitious manner over a period of time, in circumstances in which such a person or group of persons has no reasonable expectation of privacy. Monitoring is surreptitious when it is conducted in a manner designed to keep the subject of the monitoring unaware of the monitoring.

UNCLASSIFIED

- G. **Consent**: An agreement within a specific time frame and context by a person or organization to permit a particular action affecting the person or organization. Consent is obtained in written or electronic form if possible, but it can be oral if obtaining consent in written or electronic form is not possible unless a specific form of consent is required by law or these guidelines. Consent can be implied where there is adequate notice that a certain act (e.g., entering a Federal building or facility or using a Government telephone) constitutes consent to an accompanying action (e.g., inspecting a briefcase or monitoring communications). Consent may also be implied where adequate policy has been published or otherwise articulated. The Office of the General Counsel/Intelligence Law Division will determine whether a notice or policy is adequate and lawful, before I&A takes or refrains from taking action on the basis of implied consent.
- H. **Counterintelligence**: Information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, or persons, or their agents, or international terrorist organizations or activities.
- I. **Critical Infrastructure**: Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on the Nation's economic security, public health, public safety, or any combination of those matters.
- J. **Deletion**: The removal from any files or records, whether electronic or paper copy, maintained or used for intelligence purposes.
- K. **Dissemination**: The transmission, communication, sharing, or passing of intelligence or information outside I&A by any means, including oral, electronic, or physical means. Dissemination therefore includes providing any access to information retained by I&A to persons outside I&A.
- L. **Domestic Terrorism**: *Terrorism* that is not international terrorism.
- M. **Electronic Surveillance**: The acquisition of a non-public communication by electronic means without the consent of a person who is a party to an electronic communication or, in the case of a non-electronic communication, without the consent of a person who is visibly present at the place of communication, but not including the use of radio-finding equipment solely to determine the location of a transmitter.

UNCLASSIFIED

- N. **Foreign Intelligence**: Information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, foreign persons, or international terrorists.
- O. **Foreign Power**: (1) A foreign government or any component thereof, whether or not recognized by the United States; (2) a faction of a foreign nation or nations not substantially composed of United States persons; (3) an entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments; (4) a group engaged in international terrorism or activities in preparation therefor; (5) a foreign-based political organization not substantially composed of United States persons; (6) an entity that is directed and controlled by a foreign government or governments; or (7) an entity not substantially composed of United States persons that is engaged in the international proliferation of weapons of mass destruction.
- P. **I&A Personnel**: All I&A employees, including detailees or other Government personnel acting for I&A, and contractors supporting I&A.
- Q. **Incidental Collection of USPI**: Collection of USPI that is not deliberately sought by I&A, but that is nonetheless collected. Collection of USPI that is not deliberately sought is considered incidental regardless of whether it is expected or reasonably anticipated to occur.
- R. **Intelligence Activities**: All activities that elements of the Intelligence Community are authorized to conduct pursuant to Executive Order No. 12,333, "United States Intelligence Activities," as amended July 30, 2008.
- S. **Intelligence Community**: The United States Intelligence Community as defined at Title 50, United States Code, Section 3003, "Definitions," and Section 3.5(h) of Executive Order No. 12,333, "United States Intelligence Activities," as amended July 30, 2008.
- T. **International Terrorism**: Activities that (1) involve violent acts or acts dangerous to human life that violate domestic criminal law or would violate such law if committed in the United States or a State, local, or tribal jurisdiction; (2) appear to be intended to intimidate or coerce a civilian population, to influence the policy of a government by intimidation or coercion, or to affect the conduct of a government by assassination or kidnapping; and (3) occur totally outside the United States, or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to coerce or intimidate, or the locale in which their perpetrators operate or seek asylum.

UNCLASSIFIED

- U. **Key Resources**: Publicly or privately controlled resources essential to the minimal operations of the economy and government.
- V. **Mail Cover**: The non-consensual recording of any data appearing on the outside cover of any sealed or unsealed mail matter. In this context, a “recording” means a transcription, photograph, photocopy, or other facsimile of the image of the outside cover, envelope, or wrappers of mail matter. It does not include the opening or examination of mail matter.
- W. **Major Disaster**: Any natural catastrophe (including any hurricane, tornado, storm, high water, wind-driven water, tidal wave, tsunami, earthquake, volcanic eruption, landslide, mudslide, snowstorm, or drought) or, regardless of any cause, any fire, flood, or explosion in any part of the United States, which, in the determination of the President, causes damage of sufficient severity and magnitude to warrant major disaster assistance under Title 42, United States Code, Chapter 68, “Disaster Relief,” to supplement the efforts and available resources of States, local governments, and disaster relief organizations in alleviating the damage, loss, hardship, or suffering caused thereby.
- X. **Overt Collection**: Collection that is openly acknowledged by or readily attributable to the United States Government or that would be acknowledged in response to an express inquiry. Acknowledgment may include advising of United States Government affiliation (confirming the collector’s affiliation with an intelligence element is not required, so long as United States Government affiliation is acknowledged) or advising of a general collection activity applicable to that individual (rather than advising of specific acquisition methods, sites, or processes being used, or other details about the collection). For example, I&A might conduct physical surveillance at a DHS facility based on notice to I&A employees, but it would not need to notify a particular employee that he or she was the subject of the surveillance.
- Collection conducted under circumstances where, although there has been no express inquiry, it would be misleading not to disclose affiliation with the United States Government (*e.g.*, collection through observation or elicitation at an event designed for or mostly attended by a private sector audience) is only overt where the collector affirmatively discloses his or her affiliation with the United States Government.
- Y. **Physical Surveillance**: The deliberate observation of an individual to track his or her movement or other physical activities while they are occurring under circumstances in which a person has no reasonable expectation of privacy.
- Z. **Publicly Available Information**: Information that has been published or broadcast for public consumption, is available on request to the public, is accessible on-line or otherwise to the public, is available to the public by subscription or purchase, could be seen or heard by any casual observer, is made available at a meeting open to the

UNCLASSIFIED

public, or is obtained by visiting any place or attending any event open to the public.

Social media sites, Internet sites, chat rooms, bulletin boards, and other electronic and other fora, or portions of the same, belonging to individuals or groups that limit access by use of criteria that cannot generally be satisfied by members of the public are not publicly available sources.

- AA. ***Reasonable Belief***: A belief based on facts and circumstances such that a reasonable person would hold that belief. A reasonable belief must rest on facts and circumstances that can be articulated; “hunches” or intuitions are not sufficient. A reasonable belief can be based on experience, training, and knowledge as applied to particular facts and circumstances, and a trained and experienced intelligence professional can hold a reasonable belief that is sufficient to satisfy these criteria when someone lacking such training or experience would not hold such a belief.
- BB. ***Retention***: The maintenance or storage of intelligence or information. Intelligence or information that is accessed (e.g., intelligence or information on the Internet or accessible through a shared repository), but is not saved or memorialized in some manner (including in the form of summaries, reports, or notes), is not retained.
- CC. ***Shared Repository***: A database, environment, or other repository maintained for the use of more than one entity. A database, environment, or other repository that a contractor or other entity maintains solely for the use of I&A, or those acting on its behalf, is not a shared repository.
- DD. ***Terrorism***: Any activity that (1) involves an act that (a) is dangerous to human life or potentially destructive of critical infrastructure or key resources; and (b) is a violation of the criminal laws of the United States or of any State or other subdivision of the United States; and (2) appears to be intended (a) to intimidate or coerce a civilian population; (b) to influence the policy of a government by intimidation or coercion; or (c) to affect the conduct of a government by mass destruction, assassination, or kidnapping.
- EE. ***United States Person***: (1) A United States citizen, (2) an alien known by I&A to be a permanent resident alien (i.e., lawful permanent resident), (3) an unincorporated association substantially composed of United States citizens or permanent resident aliens, or (4) a corporation incorporated in the United States, except for a corporation directed and controlled by a foreign government or governments. In determining whether an unincorporated association affiliated with a foreign-based international organization is substantially composed of United States citizens or permanent resident aliens, the membership of the entire international organization is considered if the association operates directly under the control of the international organization and has no independent program or activities in the United States, but only the

UNCLASSIFIED

membership of the organization within the United States is considered if the organization within the United States conducts programs or engages in activities separate from or in addition to those directed by the international affiliate.

- FF. ***United States Persons Information (USPI)***: Information that is reasonably likely to identify one or more specific United States Persons. USPI may be either a single item of information or information that, when combined with other available information, is reasonably likely to identify one or more specific United States Persons. Determining whether information is reasonably likely to identify one or more specific United States Persons requires a case-by-case assessment by a trained intelligence professional. It is not limited to any single category of information or technology.

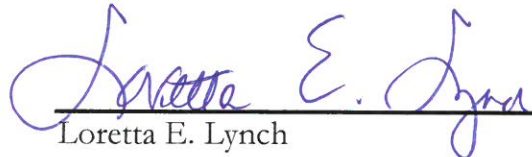
UNCLASSIFIED

APPROVAL

We approve the foregoing Guidelines in accordance with Executive Order No. 12,333, as amended.



Jeh Charles Johnson
Secretary
U.S. Department of Homeland Security



Loretta E. Lynch
Attorney General
U.S. Department of Justice

January 4, 2017

Date

January 11, 2017

Date

APPROVAL-1

UNCLASSIFIED