

**Department of Homeland Security  
Office of Intelligence and Analysis  
Instruction: IA-1000  
Revision Number: 00  
Issue Date: 01/19/2017**

# **OFFICE OF INTELLIGENCE AND ANALYSIS INTELLIGENCE OVERSIGHT PROGRAM AND GUIDELINES**

---

## **I. Purpose**

This Instruction establishes the Intelligence Oversight Program for the Office of Intelligence and Analysis (I&A) and implements the Intelligence Oversight Guidelines, as required by Executive Order 12333, "United States Intelligence Activities," as amended July 30, 2008, for the collection, retention, and dissemination of information concerning United States Persons.

## **II. Scope**

This Instruction applies to all I&A employees, including detailees or other Government personnel acting for I&A, and contractors supporting I&A (hereafter "I&A personnel"). It supersedes the memorandum, "Interim Intelligence Oversight Procedures for the Office of Intelligence & Analysis," April 3, 2008.

## **III. References**

- A. Title 50, United States Code (U.S.C.), Section 3091, "General congressional oversight provisions."
- B. Title 50, United States Code (U.S.C.), Section 3092, "Reporting of intelligence activities other than covert actions."
- C. Executive Order 12333, "United States Intelligence Activities," as amended July 30, 2008.
- D. Executive Order 13462, "President's Intelligence Advisory Board and Intelligence Oversight Board," as amended November 2, 2009.
- E. DHS Delegation 08503, "Delegation to the Under Secretary for Intelligence and Analysis/Chief Intelligence Officer," August 10, 2012.
- F. DHS Directive 252-01, "Organization of the Department of Homeland Security," March 31, 2009.

UNCLASSIFIED

- G. Department of Homeland Security Designation, "Designation of the Office of the General Counsel to Submit Reports to the President's Intelligence Oversight Board in Accordance with Executive Order 13462," August 25, 2015.
- H. Memorandum from Charles E. Allen, Under Secretary for Intelligence and Analysis, and Matthew L. Kronisch, Associate General Counsel (Intelligence), "Interim Intelligence Oversight Procedures for the Office of Intelligence & Analysis," April 3, 2008.
- I. Newly signed IO Guidelines, January 4, 2017 (Secretary Jeh Johnson), and January 11, 2017 (Attorney General Loretta E. Lynch).
- J. Intelligence Community Directive 102, "Process for Developing Interpretive Principles and Proposing Amendments to Attorney General Guidelines Governing the Collection, Retention, and Dissemination of Information Regarding U.S. Persons," November 19, 2007.
- K. Intelligence Community Directive 107, "Civil Liberties and Privacy," August 31, 2012.
- L. Intelligence Community Directive 112, "Congressional Notification," November 16, 2011.
- M. Memorandum from James R. Clapper, Director of National Intelligence, "Intelligence Community Reporting of Matters to the Intelligence Oversight Board," April 25, 2012.
- N. Memorandum from James R. Clapper, Director of National Intelligence, "Guidelines on Reporting Violations of Law or Executive Order," September 5, 2015.
- O. Memorandum from Neal S. Wolin, Chairman, Intelligence Oversight Board, "Intelligence Oversight Board's Concept of Operations," June 2, 2015.
- P. Memorandum of Understanding: Reporting of Information Concerning Federal Crimes, August 22, 1995.

## IV. Definitions

- A. ***Questionable Activity***: Any conduct related to an intelligence activity reasonably believed to constitute a violation of any applicable law, executive order, presidential or other directive, regulation, international or domestic agreement or arrangement, or applicable national or

departmental policy, including, but not limited to, the requirements of this Instruction with respect to I&A personnel.

- B. **Intelligence Activities**: All activities that elements of the Intelligence Community are authorized to conduct pursuant to Executive Order 12333, "United States Intelligence Activities," as amended July 30, 2008.

## V. Responsibilities

- A. The **Under Secretary for Intelligence and Analysis (USIA)**, as the Head of I&A, either directly or through designated personnel:
1. Ensures that I&A personnel conduct their activities in a manner that protects privacy, civil rights, and civil liberties; and complies with the requirements of Executive Order 12333 and this Instruction.
  2. Designates a senior staff member to serve as the I&A Intelligence Oversight Officer in accordance with ICD 107, "Civil Liberties and Privacy."
  3. Coordinates with the Inspector General, the Associate General Counsel for Intelligence, the Chief Privacy Officer, the Officer for Civil Rights and Civil Liberties, and the Intelligence Oversight Officer, as appropriate, on privacy, civil rights, and civil liberties matters relating to activities conducted by I&A personnel, and ensures that those officials and any staff reporting to those officials have access to any intelligence or information they deem necessary to perform their official duties; and
  4. Complies with the requirements for training, investigation, and reporting set forth in the Office of Intelligence and Analysis Intelligence Oversight Program ("I&A Intelligence Oversight Program") (See Appendix A).
- B. The **Intelligence Oversight Officer**:
1. Is responsible for matters involving the protection of civil liberties and privacy as they relate to activities conducted by I&A personnel, including by ensuring that the activities of I&A personnel comply with this Instruction;
  2. Complies with the requirements for training, investigation, and reporting set forth in the I&A Intelligence Oversight Program; and
  3. Executes and implements this Instruction.
- C. All **I&A personnel** comply with the requirements of this Instruction.

## VI. Content and Procedures

- A. **Conduct of Intelligence Activities:** I&A personnel are expected to maintain a high standard of professional and personal conduct, and are authorized to conduct intelligence activities only in accordance with the U.S. Constitution, Executive Order 12333, other applicable law, and the Department of Homeland Security Office of Intelligence and Analysis Intelligence Oversight Guidelines (“I&A Intelligence Oversight Guidelines”) (See Appendix B).
- B. **U.S. Persons Guidelines:** Executive Order 12333 requires that I&A may collect, retain, and disseminate information about U.S. Persons, and use certain information-gathering techniques, only in accordance with procedures established by the head of the Intelligence Community element concerned or by the head of a department containing such element, and approved by the Attorney General. The I&A Intelligence Oversight Guidelines, established by the DHS Secretary and approved by the Attorney General satisfy this requirement.
- C. **Training:** I&A personnel are required to attend training on the I&A Intelligence Oversight Guidelines in accordance with the I&A Intelligence Oversight Program.
- D. **Reporting:** I&A personnel shall report all intelligence activities that may violate the laws of the United States, applicable directives and policy, or this Instruction, in accordance with the I&A Intelligence Oversight Program.

## VII. Questions

Questions or concerns regarding this Instruction should be addressed to the Intelligence Oversight Officer.

Appendix A: DHS/I&A Intelligence Oversight Program

Appendix B: DHS/I&A Intelligence Oversight Guidelines



Francis X. Taylor

Under Secretary for Intelligence and Analysis



Date

# APPENDIX A

## OFFICE OF INTELLIGENCE AND ANALYSIS

### INTELLIGENCE OVERSIGHT PROGRAM

---

#### I. Purpose

This Appendix sets forth the Intelligence Oversight Program for the Office of Intelligence and Analysis (I&A).

#### II. Responsibilities

- A. The **Under Secretary for Intelligence and Analysis (USIA)**, as the Head of I&A, either directly or through designated personnel:
1. Reports through the Associate General Counsel for Intelligence to the Attorney General possible violations of Federal criminal laws by I&A personnel and of specified Federal criminal laws by any other person in a manner consistent with the protection of intelligence sources and methods;
  2. Reports through the Associate General Counsel for Intelligence to the Intelligence Oversight Board, consistent with Executive Order 13462, "President's Intelligence Advisory Board and Intelligence Oversight Board," as amended November 2, 2009, and providing copies of all such reports to the Director of National Intelligence, concerning any intelligence activities of I&A that the USIA has reason to believe may be unlawful or contrary to executive order or presidential directive;
  3. Reports through the Office of Legislative Affairs to the intelligence committees of the Congress, among other things:
    - a. Any intelligence activities of I&A that the USIA believes to be a violation of United States law, including any corrective action take or planned in connection with such activity;
    - b. Any significant misconduct by an I&A employee or contractor supporting I&A that is likely to seriously affect intelligence activities or is otherwise of congressional concern, and
    - c. Any other serious violations of United States criminal law by an I&A employee or contractor supporting I&A which, in the discretion of the USIA, warrants congressional notification;

UNCLASSIFIED

4. Coordinates with the Inspector General, the Associate General Counsel for Intelligence, the Chief Privacy Officer, the Officer for Civil Rights and Civil Liberties, and the Intelligence Oversight Officer, as appropriate, on privacy, civil rights, and civil liberties matters relating to activities conducted by I&A personnel;
5. Ensures that the Inspector General, the Associate General Counsel for Intelligence, the Chief Privacy Officer, the Officer for Civil Rights and Civil Liberties, and the Intelligence Oversight Officer, and any staff reporting to those officials, have access to any intelligence or information they deem necessary to perform their official duties;
6. Affords any aggrieved individual the opportunity for complaint, investigation, and redress of alleged violations of privacy, civil rights, or civil liberties regarding I&A's activities; and
7. Ensures that I&A personnel are properly trained in and comply with the requirements of Executive Order 12333, "United States Intelligence Activities," as amended July 30, 2008, and this Instruction.

B. The **Intelligence Oversight Officer**:

1. Develops and conducts training on the I&A Intelligence Oversight Guidelines;
2. Conducts, in coordination with the Associate General Counsel for Intelligence, as appropriate, preliminary inquiries concerning questionable activities;
3. Immediately reports the initiation of preliminary inquiries concerning known or suspected violations of Federal criminal law to the Associate General Counsel for Intelligence;
4. Reports the results of preliminary inquiries concerning all questionable activities to the USIA and the Associate General Counsel for Intelligence for referral, as appropriate, to the Inspector General, the Chief Security Officer, the President's Intelligence Oversight Board, and the Congress;
5. To the extent appropriate in light of their respective departmental responsibilities, reports the results of preliminary inquiries to the Assistant Secretary for Policy, the Chief Privacy Officer, and the Officer for Civil Rights and Civil Liberties;
6. Informs the Chief Privacy Officer and the Officer for Civil Rights and Civil Liberties of any departures by the USIA from the Department of Homeland

Security I&A Intelligence Oversight Guidelines (“I&A Intelligence Oversight Guidelines”) (See Appendix), as appropriate; and

- C. All ***I&A personnel*** comply with the requirements of this Instruction.

### III. Content and Procedures

- A. ***Training:*** I&A personnel are required to attend training on the I&A Intelligence Oversight Guidelines within thirty days of commencing employment at I&A and at least once per calendar year thereafter.
- B. ***Compliance Reviews:*** The Intelligence Oversight Officer conducts periodic reviews to verify compliance with the I&A Intelligence Oversight Guidelines. These compliance reviews include, but are not limited to, unannounced reviews (i.e., “spot checks”), reviews of audit logs, records reviews, and employee and contractor interviews. I&A personnel are required to support any compliance reviews and evaluations to the maximum extent possible.
- C. ***Reporting Requirement:*** To ensure the integrity of the intelligence profession, I&A personnel who become aware of an actual or potential violation of Federal criminal law or questionable activity are required to report the matter to the Intelligence Oversight Officer or the Associate General Counsel for Intelligence immediately.
- D. ***Prohibition on Retaliation:*** I&A personnel are prohibited from subjecting other individuals who have reported a violation of Federal criminal law or other questionable activity to any adverse action or other form of personnel action as a reprisal based upon the reporting of the questionable activity.
- E. ***Access to Information:*** The Intelligence Oversight Officer and the Associate General Counsel for Intelligence are authorized to have access to any information or intelligence necessary to perform their duties described herein.
- F. ***Preliminary Inquiry:*** Upon notification of any potential violation of Federal criminal law or questionable activity, the Intelligence Oversight Officer, in consultation with the Associate General Counsel for Intelligence, commences a preliminary inquiry.
1. If, during the inquiry, the Intelligence Oversight Officer determines there is reason to suspect a violation of Federal criminal law, he or she immediately provides notice to the Associate General Counsel for Intelligence for referral, as appropriate, to the Inspector General, the Chief Security Officer, the Attorney General, and/or the Congress.

UNCLASSIFIED

- a. Upon provision of notice of a suspected violation of Federal criminal law, the Intelligence Oversight Officer suspends the preliminary inquiry except to the extent that the Associate General Counsel for Intelligence requests his or her assistance.
  - b. Any actions taken by the Intelligence Oversight Officer concerning a suspected violation of Federal criminal law are undertaken subject to the guidance and direction of the Associate General Counsel for Intelligence.
2. Notice of any preliminary inquiry into a questionable activity is provided to the USIA and the Associate General Counsel for Intelligence for referral, as appropriate, to the Inspector General and Chief Security Officer within five business days of initiation of the inquiry unless the inquiry gives rise to a reasonable belief that the questionable activity constitutes a violation of Federal criminal law, in which case such notice is provided immediately.
  3. Notice of any preliminary inquiry giving rise to a reasonable belief that an individual has engaged in an intelligence activity that violates an international obligation, arrangement, or agreement applicable to the Department is also provided to the Assistant Secretary for Policy no later than two working days from the date on which the reasonable belief is formed.
  4. Notice of any preliminary inquiry giving rise to a reasonable belief that an individual has engaged in an intelligence activity that violates national or departmental policy concerning privacy or civil rights or civil liberties is provided to the Chief Privacy Officer, the Officer for Civil Rights and Civil Liberties, and the Associate General Counsel for Intelligence no later than two working days from the date on which the belief is formed.
- G. ***Facilitation of External Reporting:*** The Intelligence Oversight Officer facilitates the reporting of questionable activities to appropriate external entities as set forth below.
1. **Violations of Federal Criminal Law:** The Intelligence Oversight Officer reports possible violations of Federal criminal law to the Associate General Counsel for Intelligence for reporting in accordance with the processes and procedures established in the Memorandum of Understanding: Reporting of Information Concerning Federal Crimes, August 22, 1995, or any successor agreement.
  2. **Intelligence Oversight Violations:** The Intelligence Oversight Officer reports intelligence activities that are unlawful or contrary to executive order or presidential directive to the Associate General Counsel for



UNCLASSIFIED

Intelligence for referral to the Intelligence Oversight Board and the Director of National Intelligence.

- a. Significant or highly sensitive matters are reported immediately to the Associate General Counsel for Intelligence for expedited referral to the Intelligence Oversight Board and the Director of National Intelligence.
- b. All other I&A intelligence activities that are unlawful or contrary to executive or presidential directive are reported to the Associate General Counsel for Intelligence in a timely manner to facilitate quarterly reporting to the Intelligence Oversight Board and the Director of National Intelligence.

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

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.

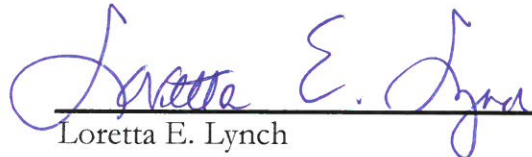


UNCLASSIFIED

**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