Department of Homeland Security
Office of Intelligence and Analysis
Policy Instruction: IA-1002
Revision Number: 00
Issue Date: 01/16/2015

SAFEGUARDING PERSONAL INFORMATION COLLECTED FROM SIGNALS INTELLIGENCE ACTIVITIES

I. Purpose

This Policy Instruction establishes the policies and procedures governing the safeguarding by Office of Intelligence and Analysis (I&A) employees of personal information collected from signals intelligence activities as required by Presidential Policy Directive-28, "Signals Intelligence Activities," January 17, 2014.

II. Scope

This Policy Instruction applies to all I&A employees (including individuals assigned or detailed to, or acting for, I&A) and contractors supporting I&A.

III. References

A. "Federal Information Security Management Act," Pub. L. No. 107-347 (codified at scattered sections of the United States Code).

B. "Federal Information Security Modernization Act of 2014," Pub. L. No. 113-283 (2014).

C. Title 6, United States Code, Chapter II, Part A, "Information and Analysis and Infrastructure Protection; Access to Information."

D. Title 50, United States Code, Section 3003, "Definitions."

E. Executive Order No. 12,333, "United States Intelligence Activities," as amended July 30, 2008.

F. Presidential Policy Directive-28, "Signals Intelligence Activities," January 17, 2014.

G. Director of Central Intelligence Directive 6/3, Annex E, "Access by Foreign Nationals to Systems Processing Intelligence Information," May 2, 2002.

H. Intelligence Community Directive No. 107, "Civil Liberties and Privacy," August 31, 2012.

I. Intelligence Community Directive No. 403, "Foreign Disclosure and Release of Classified National Intelligence," March 13, 2013.

J. Intelligence Community Directive No. 503, "Intelligence Community Information Technology Systems Security Risk Management, Certification and Accreditation," September 15, 2008.

K. Intelligence Community Policy Memorandum No. 2006-700-9, "Director of National Intelligence's Acceptance of Commonwealth Partners' Accreditation Approvals for Sovereign Information Systems Processing US National Intelligence Information," June 27, 2006.

L. National Institute for Standards and Technology Special Publication No. 800-53, "Recommended Security Controls for Federal Information Systems and Organizations," August 2009.

M. DHS Delegation No. 08503, "Delegation to the Under Secretary for Intelligence and Analysis/Chief Intelligence Officer," August 10, 2012.

N. DHS Management Directive No. 252-01, "Organization of the Department of Homeland Security," March 31, 2009.

O. Interim Intelligence Oversight Procedures for the Office of Intelligence and Analysis, April 3, 2008.

IV. Definitions

All terms used throughout this Policy Instruction are as defined in the Interim Intelligence Oversight Procedures for the Office of Intelligence and Analysis, April 3, 2008, attached hereto as "Appendix A."

V. Responsibilities

A. The ***Under Secretary for Intelligence and Analysis***, as the Head of I&A:

1. Establishes policies and procedures that apply the principles for safeguarding personal information collected from signals

intelligence activities set forth in Presidential Policy Directive-28, "Signals Intelligence Activities," January 17, 2014, and ensures that all I&A employees and contractors supporting I&A comply with the requirements of Presidential Policy Directive-28 and this Policy Instruction;

2. Ensures appropriate measures to facilitate oversight over the implementation of safeguards protecting personal information collected from signals intelligence activities; and

3. Facilitates the performance of oversight by the DHS Inspector General, the DHS General Counsel, the DHS Privacy Officer, the Officer for Civil Rights and Civil Liberties, and other relevant oversight entities, as appropriate.

B. The ***Intelligence Oversight Officer***:

1. Conducts preliminary inquiries concerning reasonably suspected violations of this Policy Instruction;

2. Immediately reports preliminary inquiries concerning known or suspected violations of Federal criminal law to the Associate General Counsel for Intelligence for referral to the DHS Inspector General and the Attorney General, as appropriate;

3. Reports other preliminary inquiries involving reported violations of this Policy Instruction to the Under Secretary for Intelligence and Analysis and the Associate General Counsel for Intelligence for referral, as appropriate, to the DHS Inspector General and the DHS Chief Security Officer, and, as appropriate, reports preliminary inquiries to the Assistant Secretary for International Affairs, the DHS Privacy Officer, and the DHS Officer for Civil Rights and Civil Liberties;

4. Informs the DHS Privacy Officer and the DHS Officer for Civil Rights and Civil Liberties of any departures from the provisions of this Policy Instruction by the Under Secretary for Intelligence and Analysis, as appropriate; and

5. Executes and implements this Policy Instruction.

C. All ***I&A employees*** and ***personnel supporting I&A*** comply with the requirements of this Policy Instruction.

VI. Content and Procedures

A. **Consistency with Law and Policy**: Pursuant to Section 1.7(i) of Executive Order No. 12,333, I&A employees and contractors supporting I&A collect (overtly or through publicly available sources), analyze, produce, and disseminate information, intelligence, and counterintelligence to support national and departmental missions. I&A employees and contractors supporting I&A are not authorized to conduct—and do not conduct—signals intelligence activities.

1. **Mission Support Requirement**: I&A employees and contractors supporting I&A retain and disseminate personal information obtained through signals intelligence only to the extent such information relates to a national or departmental intelligence requirement.

2. **Prohibition Against Activities Based Solely on Foreign Status**: I&A employees and contractors supporting I&A do not retain or disseminate information about a person obtained through signals intelligence solely because of that person's nationality or place of residence (i.e., foreign status).

B. **Retention of and Access to Personal Information Obtained through Signals Intelligence Activities**:

1. **Requirements for Retention**: I&A employees and contractors supporting I&A are authorized to retain personal information obtained through signals intelligence activities only to the extent that the retention of comparable information concerning United States Persons would be permitted under Section 2.3 of Executive Order No. 12,333, "United States Intelligence Activities," as amended July 30, 2008, and the Interim Intelligence Oversight Procedures for the Office of Intelligence and Analysis, April 3, 2008, attached hereto as "Appendix A."

a. All of the requirements of the Interim Intelligence Oversight Procedures for the permanent retention of information concerning United States Persons apply to the retention of personal information obtained through signals intelligence data.

b. Consistent with the requirements of the Interim Intelligence Oversight Procedures with respect to information concerning United States Persons, I&A employees and contractors supporting I&A are authorized to temporarily retain personal information obtained through signals intelligence activities not yet determined to qualify for permanent retention under those procedures, but only until (1) an affirmative determination is

made that the information does not qualify for permanent retention or (2) 180 days from the date on which the information is made accessible for analytic or intelligence review, whichever occurs first.

c. These protections apply regardless of the nationality of the person whose information is retained.

2. **Storage of Personal Information Obtained through Signals Intelligence Activities**: I&A employees and contractors supporting I&A store personal information obtained through signals intelligence activities under conditions that provide appropriate protection and prevent access by unauthorized persons consistent with the applicable safeguards for sensitive information contained in relevant statutes, executive orders, presidential proclamations, presidential and other directives, regulations, international and domestic agreements, arrangements, and obligations, and national and departmental policy.

a. Unclassified personal information obtained through signals intelligence activities is stored by I&A employees and contractors supporting I&A consistent with the requirements of the Federal Information Security Management Act, Pub. L. No. 107-347 (2002) (codified at scattered sections of the United States Code), the Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283 (2014), and National Institute for Standards and Technology Special Publication No. 800-53, Recommended Security Controls for Federal Information Systems and Organizations (Aug. 2009), as revised, and departmental policies and procedures implementing this guidance.

b. Classified personal information obtained through signals intelligence activities is stored by I&A employees and contractors supporting I&A consistent with the requirements of Intelligence Community Directive No. 503, Intelligence Community Information Technology Systems Security Risk Management, Certification and Accreditation (Sept. 15, 2008), and Director of Central Intelligence Directive 6/3, Annex E, Access by Foreign Nationals to Systems Processing Intelligence Information (May 2, 2002), as amended by Intelligence Community Policy Memorandum No. 2006-700-9, Director of National Intelligence's Acceptance of Commonwealth Partners' Accreditation Approvals for Sovereign Information Systems Processing US National Intelligence Information (June 27,

2006), and I&A policies and procedures implementing this guidance.

3. **Access to Personal Information Obtained through Signals Intelligence Activities**:

a. Access to personal information obtained through signals intelligence activities is limited to I&A employees and contractors supporting I&A with a need to know the information to perform an authorized mission consistent with applicable personnel security and intelligence oversight requirements as set forth in statute, executive order, presidential and other directive, and national and departmental policy.

b. I&A employees and contractors supporting I&A access personal information obtained through signals intelligence activities for which no determination has been made that the information can be permanently retained or disseminated (i.e., temporarily retained information) only to make such determinations (or to conduct authorized administrative, security, and oversight functions).

4. **Exception**: The protections set forth in Section VI.B.1-VI.B.3 of this Policy Instruction do not apply to the retention of finished intelligence products, which have already been evaluated by an element of the Intelligence Community for purposes of compliance with Presidential Policy Directive-28, "Signals Intelligence Activities," January 17, 2014; however, consistent with Section VI.A of this Policy Instruction, I&A employees and contractors supporting I&A retain such products only to the extent such information relates to a national or departmental intelligence requirement.

C. Dissemination of Personal Information Obtained through Signals Intelligence Activities:

1. **Requirements for Dissemination of Personal Information Obtained through Signals Intelligence Activities**: I&A employees and contractors supporting I&A are authorized to disseminate personal information obtained through signals intelligence activities outside I&A only to the extent such employees and contractors would be authorized to disseminate comparable information concerning United States Persons under Section 2.3 of Executive Order No. 12,333, "United States Intelligence Activities," as amended July 30, 2008, and the Interim Intelligence Oversight Procedures for the Office of Intelligence and Analysis, April 3, 2008,

attached hereto as "Appendix A." These protections apply regardless of the nationality of the person.

a. The dissemination of personal information obtained through signals intelligence activities to a foreign government is permitted only where (1) the dissemination is consistent with the interests of the United States, including the national security interests of the United States, (2) the dissemination complies with any policy guidance, treaties, or international agreements, arrangements, or obligations imposing further requirements on the dissemination or use of the information, and (3) the dissemination complies with national and Intelligence Community foreign disclosure release guidance.

b. These protections apply regardless of the nationality of the person whose information is derived from signals intelligence activities.

2. **Anonymization Requirement**: Consistent with the requirements of the Interim Intelligence Oversight Procedures with respect to information concerning United States Persons, and except as noted in Section VI.C.3 below, I&A employees and contractors supporting I&A are required to remove information identifying a person that is obtained through signals intelligence activities prior to disseminating such information unless the information is necessary for the intended recipient to understand, assess, or act on the information provided, and all I&A intelligence reports and finished analytic products containing information identifying a person that is obtained through signals intelligence activities is reviewed to determine whether inclusion is necessary for the intended recipient.

a. I&A employees and contractors supporting I&A make the determination as to whether personal information needs to be included in an intelligence report or product consistent with applicable Intelligence Community standards for accuracy and objectivity as set forth in applicable intelligence community directives, with particular care taken to apply standards relating to the quality, sensitivity, and reliability of the information, consideration of alternative sources of information and interpretations of data, and objectivity in performing analysis.

b. Where such information is unnecessary, it is replaced with a generic description of the information (i.e., "a person" for "[Person X]" or "a corporation" for "[Corporation Y]"), but without any indication in the disseminated information that personal information has been anonymized.

3. **Exception**: The protections set forth in Section VI.C.1-VI.C.2 of this Policy Instruction do not apply to the dissemination of finished intelligence products originating outside and not materially authored, amended, or altered by I&A employees or contractors supporting I&A, which have already been evaluated by an element of the Intelligence Community for purposes of compliance with Presidential Policy Directive-28, "Signals Intelligence Activities," January 17, 2014; however, consistent with Section VI.A of this Policy Instruction, I&A employees and contractors supporting I&A disseminate such products only to the extent they relate to a national or departmental intelligence requirement.

D. **Training**: I&A employees and contractors supporting I&A are required to receive training on the requirements set forth in this Policy Instruction within thirty days of commencing employment or providing contract support to I&A and at least once per year thereafter. I&A employees and contractors supporting I&A are required to receive this training in person where practicable.

E. **Compliance Reviews**: I&A employees and contractors supporting I&A are subject to periodic compliance reviews performed by the Intelligence Oversight Officer, including, but not limited to, unannounced reviews (i.e., "spot checks"), reviews of audit logs, records reviews, and employee interviews to verify compliance with the requirements of this Policy Instruction. I&A employees and contractors supporting I&A are required to support any such compliance reviews to the maximum extent possible.

F. **Reporting Violations**:

1. I&A employees or contractors supporting I&A who, in the course of performing their official duties, have reason to believe that an I&A employee or contractor supporting I&A has committed, is committing, or will commit a violation of this Policy Instruction are required to report the matter to the Intelligence Oversight Officer, the Associate General Counsel for Intelligence, or the DHS Inspector General.

    a. Notice to the Intelligence Oversight Officer, Associate General Counsel for Intelligence, or DHS Inspector General is required as soon as possible, but in no event later than two business days from the date on which that reasonable belief is formed.

    b. No I&A employee or contractor supporting I&A is permitted to subject an I&A employee or contractor supporting I&A who has reported a violation or potential violation of this Policy Instruction

to any adverse action based upon the reporting of the violation or potential violation.

2. Upon notification of any reasonably suspected violation of this Policy Instruction, the Intelligence Oversight Officer commences a preliminary inquiry to determine the facts surrounding the matter in question and, in consultation with the Associate General Counsel for Intelligence, as appropriate, assess whether the activity violates this Policy Instruction or is otherwise unlawful or contrary to Federal criminal law, executive order, presidential or other directive, regulation, international or domestic obligation, agreement, or arrangement, or national or departmental policy.

a. Notice of any preliminary inquiry into a reasonably suspected violation of Federal criminal law is provided immediately to the Under Secretary for Intelligence and Analysis and the Associate General Counsel for Intelligence for referral to the DHS Inspector General, the DHS Chief Security Officer, and the Attorney General, as appropriate.

b. Notice of any preliminary inquiry into a reported violation or potential violation of this Policy Instruction is otherwise provided to the Under Secretary for Intelligence and Analysis and the Associate General Counsel for Intelligence for referral, as appropriate, to the DHS Inspector General, the DHS Chief Security Officer, and, for significant instances of non-compliance, the Director of National Intelligence within five business days of initiation of the inquiry.

c. 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 through the Foreign Disclosure and Release Officer no later than two working days from the date on which the reasonable belief is formed.

d. 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 DHS Privacy Officer, the DHS 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. **Departures and Amendments**: Departures from or amendments to the provisions of this Policy Instruction are permitted in accordance with the requirements set forth below.

1. Except as permitted by Section VI.G.2 of this Policy Instruction, departures from or amendments to this Policy Instruction are permitted only where and to the extent authorized in advance by the Under Secretary for Intelligence and Analysis after consultation with the Office of Director of National Intelligence and the National Security Division of the Department of Justice, and notice of any departures are provided to the Intelligence Oversight Officer for referral to the DHS Privacy Officer or DHS Officer for Civil Rights and Civil Liberties, as appropriate.

2. If there is not time for such approval or consultation and a departure from this Policy Instruction is necessary because of the immediacy or gravity of a threat to the safety of persons or property or to the national security (i.e., a clear, imminent threat of such severity exists that the failure to depart from the provisions of the Policy Instruction 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 that threat), the Under Secretary for Intelligence and Analysis or his or her designee may approve a departure from this Policy Instruction.

3. Any departures from the substantive provisions of this Policy Instruction pursuant to Section VI.G.2 of this Policy Instruction are required to be reported to the Associate General Counsel for Intelligence for referral to the Assistant Attorney General for National Security and Director of National Intelligence, the Intelligence Oversight Officer for referral, as appropriate, to the DHS Privacy Officer and the DHS Officer for Civil Rights and Civil Liberties, and, where the departure is authorized by a designee of the Under Secretary for Intelligence and Analysis, to the Under Secretary for Intelligence and Analysis as soon as is practicable, but in any event no later than one working day from the authorization for departure.

4. Notwithstanding the provisions for amendment or departure set forth above, all activities conducted by I&A employees and contractors supporting I&A are required to be carried out in a manner consistent with the Constitution and the laws of the United States under all circumstances.

VII. Questions

Questions or concerns regarding this Policy Instruction should be addressed to the I&A Intelligence Oversight Officer.

Appendix A: Interim Intelligence Oversight Procedures for the Office of Intelligence and Analysis, April 3, 2008

Francis X. Taylor
Under Secretary for Intelligence and Analysis

January 16, 2015
Date

APPENDIX A:

Interim Intelligence Oversight Procedures for the Office of Intelligence and Analysis

~~UNCLASSIFIED//FOUO~~

U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

April 3, 2008

MEMORANDUM FOR: All Employees, Detailees, and Contractors Supporting the Office of Intelligence and Analysis

FROM: Charles E. Allen
Under Secretary for Intelligence and Analysis

Matthew L. Kronisch
Associate General Counsel (Intelligence)

SUBJECT: Interim Intelligence Oversight Procedures for the Office of Intelligence & Analysis[1]

Introduction

The Department of Homeland Security ("DHS" or "Department") Office of Intelligence and Analysis (I&A) is a member of the United States Intelligence Community.[2] As such, I&A is subject to Executive Order 12333, "United States Intelligence Activities," which establishes the basic tenets of Intelligence Oversight. The purpose of Intelligence Oversight is to enable I&A intelligence professionals to effectively carry out their authorized functions while ensuring that their activities affecting U.S. persons[3] are conducted in a manner that protects the constitutional rights and privacy of those U.S. persons and maintains the integrity of the intelligence profession.

Pending approval by the Attorney General of I&A's formal implementing procedures for EO 12333, this document is designed to serve as interim guidance for all I&A personnel (employees, detailees, and contractors supporting I&A) involved in intelligence activities. The guidance contained herein, however, does not substitute for legal review of specific intelligence activities, and any questions on the applicability or interpretation of this guidance should be directed to the Office of General Counsel (Intelligence).

---

[1] This memorandum revokes the memorandum, "Intelligence Oversight Basics" dated March 27, 2006.
[2] http://www.intelligence.gov; See also, § 201(h) of the Homeland Security Act of 2002, as amended, the National Security Act of 1947, a amended, and Executive Order 12333, as amended by Executive Order 13284.
[3] For purposes of Intelligence Oversight, the definition of a United States (U.S.) person includes: (a) a U.S. citizen; (b) an alien know by I&A to be a permanent resident alien; an unincorporated association substantially composed of (a) or (b); (c) a corporation incorporated in the U.S., except for a corporation directed and controlled by a foreign government(s). A corporation or corporate subsidiary incorporated abroad, even if partially or wholly owned by a corporation incorporated in the U.S., is not a U.S. person. A person or organization outside the U.S. shall be presumed not to be a U.S. person unless specific information to the contrary is obtained. A person or organization within the U.S. shall be presumed to be a U.S. person unless specific information to the contrary is obtained. However, an alien within the U.S. shall be presumed not to be a U.S. person unless I&A obtains specific information to the contrary.

In order to understand Intelligence Oversight, you must be familiar with the following core concepts:

- authorized I&A intelligence activities;
- collection of information about U.S. persons;
- retention of information about U.S. persons;
- dissemination of information about U.S. persons;
- minimization of information about U.S. persons;
- identification and reporting of Questionable Activities.

Each of these core concepts is explained below.

Authorized I&A Intelligence Activities

Employees, detailees, and contractors supporting I&A are expected to conduct only authorized intelligence activities necessary for the protection of national and homeland security and to support the mission of the Department. For I&A, authorized intelligence activities are derived primarily from Title II of the Homeland Security Act of 2002 (as amended), EO 12333 (as amended), and the National Security Act of 1947 (as amended). These authorized intelligence activities can generally be understood as falling within one of the following areas:

(1) **Specific Tasks Related to Terrorist Threats**. This category includes a number of specific activities explicitly authorized by law or presidential directive, such as conducting intelligence analysis, facilitating information and intelligence sharing, and establishing and managing collection priorities. All activities performed in this category must relate to terrorist threats to the homeland.

(2) **General Tasks Related to Priorities for Protective and Support Measures**. This category includes general activities undertaken in furtherance of identifying priorities for protective and support measures by the Department, other agencies of the Federal Government, State and local government agencies and authorities, the private sector, and other entities. An example includes integrating relevant information, analyses, or vulnerability assessments from the Intelligence Community with those from within and outside the Department. All activities performed in this category must relate to actual or potential threats to homeland security.[4]

(3) **General Tasks Related to Departmental Support**. This category includes general intelligence and information analysis and support provided to other elements of the Department. All activities performed in this category must be undertaken in furtherance of a lawful activity of the component, such as border security, immigration, or protective activities.

(4) **General Tasks Directed by the Secretary**. This category includes activities undertaken at the direction of the Secretary. All activities performed in this category must relate to a responsibility of the Department, such as serving as the Executive Agent for the National

[4] Threats to homeland security include all threats or hazards, regardless of origin, that relate to: critical infrastructure or key resources; a significant public safety, public health or environmental impact; political, societal and economic infrastructure; border security; the proliferation or use of weapons of mass destruction; or other potential catastrophic events including man-made and natural disasters.

Applications Office.

(5) **Specific Tasks Directed by Statute or Presidential Directive**. This category includes specific activities required by law or presidential directive, such as accessing and providing required information in response to a discovery request or providing training to Departmental or other personnel.

I&A personnel generally operate within a particular division of I&A with a discrete mission focus. I&A personnel are encouraged to develop a comprehensive understanding of how their intelligence activities align with the authorities framework above. Emphasis should be placed on understanding how the U.S. person rules discussed in this memo are related to the authorities that apply to their specific mission area. The Office of General Counsel (Intelligence) attorneys and the I&A Intelligence Oversight Officer are available to assist in this effort. This consultation is required when undertaking new initiatives under paragraphs 2-5, above, as well as whenever any initiative may impact constitutionally protected activities.

Collection of Information About U.S. Persons

Collection means the gathering or receipt of information, regardless of source, by I&A, coupled with an affirmative act demonstrating intent to use or retain that information for intelligence purposes.

In order to ensure both the acquisition of essential information and the protection of individual interests, I&A may collect information about U.S. persons only when 1) necessary for the conduct of an authorized I&A intelligence activity, and 2) the information is reasonably believed[5] to fall within one of the following categories.

- **Information Obtained with Consent**. The voluntary agreement by a person or organization to permit a particular action that affects the person or organization. Consent may be oral or written unless a specific form of consent is required by a particular procedure. Consent may also be implied where there is adequate notice that a certain act (e.g., entering a federal building or facility, using a government telephone) constitutes consent to an accompanying action (e.g., inspection of briefcase, monitoring of communications).
- **Publicly Available Information**. Information that has been published or broadcast in some manner to the general public; is available upon request to a member of the general public; is accessible to the public; is available to the public by subscription or purchase; could lawfully be seen or heard by a casual observer; is made available at a meeting open to the public; or is obtained by visiting any place or attending any event that is open to the public. Open Source Information is a form of Publicly Available Information.
- **Foreign Intelligence**. Information relating to the capabilities, intentions or activities of foreign governments or elements thereof, foreign organizations or foreign persons, or international terrorist activities.
- **Counterintelligence**. Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of

[5] A reasonable belief arises when the facts and circumstances are such that a reasonable person would hold the belief. Reasonable belief must rest on facts and circumstances that can be articulated; "hunches" or intuitions are not sufficient. Reasonable belief may be based upon experience, training and knowledge in intelligence or a related field, applied to the facts and circumstances at hand.

foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist organizations.

- **Potential Sources of Assistance to Intelligence Activities**. Information necessary for the purpose of determining the suitability or credibility of individuals reasonably believed to be potential sources of information or of assistance to intelligence activities.
- **Protection of Intelligence Sources and Methods**. Information needed to protect foreign intelligence or counterintelligence sources or methods from unauthorized disclosure. Within the United States, intentional collection of such information shall be limited to present or former DHS employees or detailees, present or former contractors or their present or former employees, or applicants for employment at DHS or at a contractor of DHS.
- **Personnel, Physical or Communications Security**. Information arising out of lawful personnel, physical or communications security investigations.
- **Terrorism Information**. Information relating to the existence, organization, capabilities, plans, intentions, vulnerabilities, means of finance or material support, or activities of foreign or transnational terrorist groups or individuals, domestic groups or individuals involved in 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 or individuals reasonably believed to be assisting or associating with them.
- **Vulnerabilities Information**. Information required for the protection of the key resources and critical infrastructure of the United States. Key resources under the Homeland Security Act, section 2(10), means "publicly or privately controlled resources essential to the minimal operations of the economy and government. Critical infrastructure is defined at 42 U.S.C. 5195c(e) as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." These terms are further developed in Homeland Security Presidential Directive 7 "Critical Infrastructure Identification, Prioritization and Protection."
- **International Narcotics Activities**. Activities to create, manufacture, distribute, or dispense, or possess with intent to create, manufacture, distribute, or dispense a controlled substance in violation of law, conducted at least in part outside the territorial jurisdiction of the United States.
- **Border Security Information**. Information necessary to protect the safety and integrity of our borders, including information about persons believed to be engaged in activities intended to violate immigration and customs laws and regulations.
- **Threats to Safety**. Information needed to protect the health or safety of any person or organization. Examples include information that may be necessary to identify priorities for either protective security measures or emergency preparedness and response activities, by the Department, other government agencies, the private sector, and other entities.
- **Overhead Reconnaissance**. Information collected from overhead reconnaissance not directed at specific U.S. persons. The collection, retention and dissemination of domestic Overhead Reconnaissance information raise numerous legal and policy issues. Any planned collection or dissemination of domestic Overhead Reconnaissance information must be approved by the Office of General Counsel (Intelligence).

- **Administrative Information**. Information necessary for the functioning of the Office of Intelligence and Analysis but not directly related to the performance of authorized intelligence activities. Such information would include DHS personnel and training records, reference materials, contractor performance records, public and legislative affairs files, and correspondence files maintained in accordance with applicable directives.

Retention of Information About U.S. Persons

Retention means the maintenance, storage, synthesis, analysis, production, and other uses short of dissemination, of information about United States persons that can be retrieved by reference to the U.S. person's name or other personally identifying information.

I&A may retain information regarding U.S. persons, without their consent, only if the information was properly collected and only when it is necessary to the conduct of an authorized I&A intelligence activity. The following principles must be observed to ensure information is properly retained:

- **Temporary retention**. Information about U.S. persons may be retained temporarily, for a period not to exceed 180 days, solely for the purpose of determining whether that information may be permanently retained under these guidelines. Once the holder of the information determines that information may not be retained, the U.S. person identifying information is to be destroyed immediately.
- **Forwarding information**. If the information, although not authorized for retention by I&A, is potentially relevant to the responsibilities of another IC element, consideration should be given to forwarding the information to the other element, consistent with all applicable laws, executive orders, or regulations.
- **Incidentally acquired information**. Information about U.S. persons acquired incidental to authorized collection may only be retained if such information could have been collected intentionally and only when it is necessary to the conduct of an authorized I&A intelligence activity.
- **Access to retained information**. Access within I&A to information about U.S. persons shall be limited to those individuals who have a need for the information in order to perform their official duties.
- **Review of intelligence records**. All I&A personnel shall conduct an annual review of their intelligence records (in whatever form they may be maintained) in order to evaluate and ensure that continued retention of the U.S. person information is necessary to the conduct of an authorized I&A intelligence activity.
- **Exceptions.** The foregoing requirements do not apply to information retained solely for administrative purposes or information retained in compliance with an independent legal requirement.
- **Freedom of Information Act and the Privacy Act Applicability.** The Freedom of Information Act (5 U.S.C. § 552) and the Privacy Act (5 U.S.C. § 552a) apply to all U.S. person information retained by I&A.

Dissemination of Information About U.S. Persons

Dissemination means the transmission, communication, sharing, or passing of information outside of I&A, or to any individual not otherwise assigned to or directly supporting I&A.

I&A may disseminate information regarding U.S. persons, without their consent, only under any of the following three conditions:[6]

1. Where information, although not authorized for retention by I&A is potentially relevant to the responsibilities of another IC element, the information may be forwarded to the other element, consistent with all applicable laws, executive orders, or regulations;[7] or
2. Where dissemination is required by an independent legal authority and is not undertaken as an intelligence or information sharing activity; or
3. To appropriate Federal, State, tribal, and local government agencies and authorities, the private sector, and other entities, so long as the information was properly collected and/or retained, and, there exists a reasonable belief that the intended recipient of the information has a need to receive such information for the performance of a lawful governmental or homeland security function, such as:

- An employee of a law enforcement intelligence or non-intelligence component of DHS who has a need to know the information to perform his or her official duties;
- A federal, state, tribal or local law enforcement entity when the information indicates violation of laws enforced by the law enforcement entity;
- An agency of a state or local government, or a private sector entity with responsibilities relating to homeland security, in order to assist in the deterrence, prevention, preemption of, or response to, terrorist attacks against the U.S.;
- A protective, immigration, national defense, or national security agency of the federal government authorized to receive such information in the performance of a lawful governmental function;
- A foreign government and dissemination is undertaken pursuant to an agreement or other understanding with such government in accordance with applicable foreign disclosure policies and procedures.

Non-publicly available information about U.S. persons obtained through court-authorized electronic surveillance and physical searches should not be provided to state, local, or private sector authorities unless it is confirmed that the information is not FISA-derived, does not concern a U.S. person, or is otherwise to be provided in conformance with court-approved procedures.

Any dissemination of U.S. person information that does not conform to the conditions set forth above requires the approval of the Under Secretary for Intelligence and Analysis after consultation with the Office of General Counsel (Intelligence).

---

[6] Any dissemination of classified intelligence must be done consistent with E.O. 13292, *Further Amendment to Executive Order 12958, as Amended, Classified National Security Information* , E.O. 12968, *Access to Classified Information*, and E.O. 13388, *Further Strengthening the Sharing of Terrorism Information To Protect Americans.*

[7] This does not include information derived from signals intelligence or otherwise collected originally pursuant to the Foreign Intelligence Surveillance Act, which may only be disseminated in accordance with applicable directives and procedures, including any court-approved procedures, specifically addressing each of these types of information.

Minimization

I&A personnel shall not disseminate information identifying a U.S. Person unless such data is deemed necessary for the intended recipient to understand, assess, or act on the information provided. Prior to any dissemination of U.S. person information, the information is to be reviewed to determine whether inclusion is necessary for the intended recipient. This review process is called "minimization." Products intended for multiple recipients may require tailored versions, each with varying degrees of U.S. person identifying information, based upon the respective intended audience for each product.

- When not necessary, the personally identifying information will be replaced with "a U.S. Person," "USPER," "a U.S. Corporation," etc., as appropriate. The product will indicate through an advisory that the information has been minimized and inform recipients how they may obtain the U.S. person information should their mission require it.

- When it is necessary for a product to include U.S. person information, the product must indicate the presence of this information through an advisory such as "this product contains U.S. person information" or words to that effect. Additionally, the U.S. person information should be highlighted in some manner that clearly indicates that it is considered U.S. person information.

Identifying and Reporting Questionable Activities

A questionable activity is any conduct by I&A personnel that may constitute a violation of the law, any Executive Order or Presidential Directive, or these guidelines. It includes professional and personal violations of any federal criminal law.

I&A intelligence personnel are expected to maintain a high standard of professional and personal conduct. I&A intelligence personnel are authorized to conduct intelligence activities only in accordance with EO 12333 and these interim procedures. They are not to exceed the authorities granted to I&A by law, executive order, or regulation. To ensure the integrity of the intelligence profession and avoid exceeding I&A authorities, I&A personnel who are aware of an actual or potential questionable activity are required to immediately report the matter to either the I&A Intelligence Oversight Officer, the Office of General Counsel (Intelligence), or the Inspector General.

Conclusion

As mentioned above, these procedures are designed to serve as a reference tool for all I&A personnel involved in intelligence activities. It does not substitute for legal review of specific intelligence activities, and any questions on the applicability or interpretation of thse procedures should be directed to the legal staff.

These procedures are set forth solely for tbe purpose of internal DHS I&A guidance. They do not create any rights, substantive or procedural, enforceable by law by any other party in any civil or criminal matter, nor does it place any limitation on otherwise lawful investigative and litigative prerogatives of the U.S. Government.