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 — January 16, 2015

Francis X. Taylor
Under Secretary for Intelligence and Analysis

Date

Department of Homeland Security
Office of Intelligence and Analysis
Policy Instruction: IA-900
Revision Number: 01
Issue Date: 01/13/2015

OFFICIAL USAGE OF PUBLICLY AVAILABLE INFORMATION

I. Purpose

This Instruction establishes the standards, guidelines, and processes for using Publicly Available Information, including publicly available social media platforms, for research, collection, analysis, retention, citing, reporting, and dissemination within the Office of Intelligence and Analysis (I&A).

II. Scope

This Instruction applies to all I&A personnel, including detailees and contractors.

III. References

A. The Antideficiency Act, 31 U.S.C §§ 1341-54.

B. The Copyright Act of 1976, Pub. L. 94-553, 90 Stat. 2541, as amended.

C. Intelligence Community Directive 206, "Sourcing Requirements for Disseminated Analytic Products," October 17, 2007.

D. DHS Directive 110-01, "Privacy Policy For Operational Use of Social Media," June 8, 2012.

E. DHS Directive 4300A, "Sensitive Systems Handbook," July 24, 2012.

F. DHS Policy Directive 8310, "Request for Information (RFI)," February 21, 2007.

G. DHS Instruction 110-01-001, "Privacy Policy For Operational Use of Social Media," June 8, 2012.

H. Office of Management and Budget Memorandum, "Antideficiency Act Implications of Certain Online Terms of Service Agreements," April 4, 2013.

I. I&A Memorandum, "Interim Intelligence Oversight Procedures for the Office of Intelligence and Analysis," April 3, 2008 ("Intelligence Oversight Procedures").

IV. Definitions

A. ***Collection***: 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. Research is a form of collection.

B. ***Dissemination***: The transmission, communication, sharing or passing of an I&A Product to any federal, state, local, tribal, or territorial government, private sector entity, or any foreign government, foreign person, or international organization, including by e-mail, hard copy, posting to web sites, or any other method of distribution.

C. ***Homeland Security Standing Information Needs (HSEC SINs)***: Enduring all-threats and all-hazards information needs of DHS and its federal, state, local, tribal, territorial, and private sector stakeholders and other homeland security partners. HSEC SINs are gathered, integrated, and maintained by I&A and form the foundation for information collection activities within I&A.

D. ***I&A Products***: The physical manifestation, regardless of form or format, of analytic efforts conducted in furtherance of the I&A mission, which represent the analytic assessment, judgment, or other analytic input of I&A or intelligence personnel, and which are intended for Dissemination. Not included are the informal sharing* of raw or unevaluated information, analyst-to-analyst exchanges, products issued by Intelligence Watch and Warning that may contain limited analytic content, or the sharing of third party products.

E. ***Open Source***: Unclassified information that has been published or broadcast in some manner to the general public, 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.

F. ***Open Source Information Report (OSIR)***: A raw report containing information that has been acquired as a result of Collection from a publicly available source, including but not limited to Open Source and Social Media, prior to any interpretation or analysis.

G. ***Publicly Available Information***: Unclassified information that has been published or broadcasted in some manner to the general 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

* Informal sharing is distinct from formal Dissemination in that it does not result in a finished analytical product being made available broadly outside of the federal government through posting to web sites or distribution via e-mail.

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.

H. ***Request for Information (RFI)***: A validated expression of need for information. The informal, personal exchange of ideas or concepts by analysts, operators, or subject matter experts to further increase their personal understanding of an event, situation, or problem set are considered analytic exchanges and not RFIs.

I. ***Research***: The collection of information or intelligence by I&A personnel for the purpose of improving the understanding of a topic or subject of analytic interest.

J. ***Social Media***: The sphere of websites, applications, and web-based tools that connect users to engage in dialogue, share information and media, collaborate, and interact. Social Media takes many different forms, including but not limited to web-based communities and hosted services, social networking sites, video and photo sharing sites, wikis, blogs, virtual worlds, social bookmarking, and other emerging technologies.

V. Responsibilities

A. The ***Head of I&A Information Compliance/Intelligence Oversight Officer*** oversees and directs the execution of all functions performed by I&A Information Compliance, including with respect to the oversight of I&A's collection, retention, and dissemination of information or intelligence from publicly available sources, in order to ensure compliance with Intelligence Oversight Procedures and facilitate corrective action in the case of discrepancies or non-compliance.

B. The ***I&A Privacy Officer*** is the I&A official primary responsible for privacy compliance and policy, including with respect to the collection, retention, and dissemination of information or intelligence from publicly available sources, acting in coordination with the DHS Chief Privacy Officer and the Office of the General Counsel, Intelligence Law Division (OGC-ILD), and subject to the guidance and direction of I&A Information Compliance/Intelligence Oversight Officer.

C. The ***Intelligence Support and Integration Division Chief*** is responsible for all research-related activities conducted in accordance with this policy, including all such activities conducted by the I&A Supervisors of Open Source Reviewers.

D. The ***Head of I&A Collection Operations*** oversees and directs the execution of all functions performed by I&A Collection Operations, which includes

ensuring the content review of I&A Collection Operation's open source reporting and, in coordination and consultation with the I&A Intelligence Oversight Officer and OGC-ILD, establishing training requirements, including training in privacy, civil rights and civil liberties, intelligence oversight, applicable legal authorities, and operational security tradecraft and technology, for Open Source Officers and Open Source Specialists.

E. The ***Head of I&A Training***, in coordination and consultation with I&A Collection Operations, the I&A Intelligence Oversight Officer, OGC-ILD, and other relevant I&A officials, establishes training requirements, including training in privacy, civil rights and civil liberties, intelligence oversight, applicable legal authorities, and operational security tradecraft and technology, for Open Source Reviewers.

F. ***I&A Supervisors of Open Source Reviewers***:

1. Validate their respective I&A personnel's job-related duties prior to approving a request to become an Open Source Reviewer;

2. Confirm training requirements and compliance procedures are satisfied prior to approving a request to become an Open Source Reviewer;

3. Oversee and direct the execution of all functions and compliance procedures performed by their Open Source Reviewers; and

4. Maintain social media platform registration records and, as requested, provide such records to I&A Collection Operations for collection and operational de-confliction.

G. ***Open Source Officers (OSOs)***:

1. Collect and retain information or intelligence from publicly available sources, including publicly available social media platforms maintained and/or provided by non-Federal government entities, in response to established HSEC SINs, validated RFIs, and/or other validated intelligence requirements;

2. Disseminate information or intelligence collected from publicly available sources, including publicly available social media platforms maintained and/or provided by non-Federal government entities, via OSIRs or other appropriate reporting channels;

3. Coordinate the review of open source reporting, including OSIRs, by I&A Collection Operations with I&A Information Compliance, and, where appropriate, OGC-ILD; and

4. Directly oversee Open Source Specialists' collection, retention, and dissemination of information or intelligence from publicly available sources, including publicly available social media platforms maintained and/or provided by non-Federal government entities.

H. ***Open Source Specialists (OSSes)***:

1. Collect and retain information or intelligence from publicly available sources, including publicly available social media platforms maintained and/or provided by non-Federal government entities, in response to established HSEC SINs, validated RFIs, and/or other validated intelligence requirements; and

2. Disseminate information or intelligence collected from publicly available sources, including publicly available social media platforms maintained and/or provided by non-Federal government entities, via OSIRs or other appropriate reporting channels.

I. ***Open Source Reviewers (OSRs)*** review and conduct research from publicly available social media platforms maintained and/or provided by non-Federal government entities, and, when appropriate, refer those results to I&A Collection Operations for collection and reporting.

VI. Content and Procedures

A. ***Content***

1. *Consistency with Law and Policy*: All collection (including research), analysis, retention, reporting, and dissemination of information or intelligence derived from publicly available sources, including publicly available social media platforms, by I&A personnel is performed in accordance with the Constitution and all applicable statutes, executive orders, regulations, presidential and other directives, national and departmental policies, and international obligations.

2. *I&A Access to Publicly Available Information*: In furtherance of an authorized I&A activity, all I&A personnel are permitted to collect, retain, analyze, disseminate and cite information or intelligence in I&A Products from publicly available sources, except from publicly available social media platforms maintained and/or provided by non-Federal government entities.

   a. In furtherance of their professional I&A responsibilities, I&A personnel do not use personal accounts/registrations to access publicly available information, including information from publicly available social media platforms.

b. All sourcing and citing of publicly available information is performed in accordance with ICD 206, as applicable.

3. *I&A Access to Social Media Platforms Maintained by the Federal Government*: In furtherance of an authorized I&A activity, all I&A personnel use publicly available social media platforms and services maintained and/or provided by the Federal government to coordinate and collaborate with other Intelligence Community elements and Federal, State, local, tribal, territorial, private sector and other homeland security partners, as appropriate.

4. *I&A Access to Other Social Media Platforms*: In furtherance of an authorized I&A activity, OSOs, OSSes, and OSRs are permitted to access publicly available social media platforms maintained and/or provided by non-Federal government entities in accordance with the following requirements and restrictions:

   a. OSOs, OSSes, and OSRs, in coordination and consultation with the I&A Intelligence Oversight Officer and OGC-ILD, obtain user accounts with publicly available social media platforms maintained and/or provided by non-Federal government entities.

   b. OSOs, OSSes, and OSRs only register and/or create user accounts with publicly available social media platforms maintained and/or provided by non-Federal government entities that do not require human interaction during the registration or reviewing process.

   c. OSOs, OSSes, and OSRs do not engage any social media participants. Examples of engagement include, but are not limited to, "friending," interviewing, chatting, or posting. If engaged by any online user, OSOs, OSSes, and OSRs withdraw from the social media platform immediately.

   d. OSOs, OSSes, and OSRs record all their user accounts/registrations with publicly available social media platforms maintained and/or provided by non-Federal government entities, and, in accordance with Intelligence Community policies, standards, and guidelines, coordinate and de-conflict their social media accounts with other Intelligence Community elements or law enforcement community personnel.

5. *Terms of Service/User Agreements*: I&A personnel do not enter into agreements or arrangements (including terms of service or user agreements) with publicly available sources, including publicly available social media platforms, in a manner that is incompatible with Federal law, regulation, and/or policy, including the Anti-Deficiency Act. In the course of

registering or otherwise accepting access to publicly available sources, including publicly available social media platforms, I&A personnel do not agree or otherwise consent to terms of services or user agreements that contain unrestricted, open-ended indemnification provisions/clauses.

6. *Copyright Protected Materials*: I&A personnel reproduce copyrighted works and materials in accordance with Federal law, regulations, and policies, including the Copyright Act of 1974, as amended. I&A personnel direct all questions and concerns related to the Copyright Act of 1974, as amended, to OGC-ILD.

7. *Acquisitions and Procurement*: I&A personnel, after coordination with the I&A Chief Financial Officer, the I&A Intelligence Oversight Officer, and their respective Division Directors, procure or acquire fee-based services from publicly available sources. I&A personnel do not access "free trial offer" services from publicly available sources, unless approved by their Division Directors, after coordination and consultation with the I&A Chief Financial Officer, the I&A Intelligence Oversight Officer, and OGC-ILD.

B. ***Process***:

1. In furtherance of an authorized I&A activity, OSRs, OSOs, and OSSes access publicly available social media platforms maintained and/or provided by non-Federal government entities in accordance with the following framework:

   a. *OSRs*:

      i. I&A personnel submit formal written requests to become OSRs to their supervisors.

      ii. OSRs receive mandatory training in privacy, civil rights and civil liberties, intelligence oversight, applicable legal authorities, and operational security tradecraft and technology prior to being permitted to review and research information or intelligence from publicly available social media platforms maintained and/or provided by non-Federal government entities.

      iii. OSRs review and research information or intelligence determined to be mission-relevant from publicly available social media platforms maintained and/or provided by non-Federal government entities. OSRs may refer such information or intelligence to an OSO and/or OSSes for collection and reporting using established protocols and procedures, such as through RFIs. Once the referral/RFI is validated and the information or intelligence is reported and disseminated by an OSO or OSS, the OSR is

permitted to use the reported information or intelligence for formal analysis and/or intelligence production.

1. OSRs are permitted to conduct research from publicly available social media platforms maintained and/or provided by non-Federal government entities only within the scope of an established HSEC SIN.

2. Information or intelligence obtained through research from publicly available social media platforms maintained and/or provided by non-Federal government entities may not be used in intelligence products or for intelligence production absent formal collection and reporting, as appropriate.

b. *OSOs and OSSes*:

i. OSOs and OSSes are authorized to collect, retain, report and disseminate information or intelligence from publicly available social media platforms maintained and/or provided by non-Federal government entities.

ii. OSOs and OSSes receive mandatory training established by I&A Collection Operations in privacy, civil rights and civil liberties, intelligence oversight, applicable legal authorities, and operational security tradecraft and technology prior to being permitted to review information or intelligence from publicly available social media platforms maintained by non-Federal government entities.

2. For guidance on the use of publicly available information for non-intelligence purposes, I&A personnel refer to established policies, procedures, and guidelines, such as those in DHS 4300A, Sensitive Systems Handbook.

VII. Questions

Questions or concerns regarding this policy should be addressed to the Plans, Policy, and Management Division.

Francis X. Taylor
Under Secretary for Intelligence and Analysis

1/13/15
Date