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