Department of Homeland Security
DHS Directives System
Instruction Number: 110-01-001
Revision Number: 00
Issue Date: 6/8/2012

PRIVACY POLICY FOR OPERATIONAL USE OF SOCIAL MEDIA

I. Purpose

This Instruction implements Department of Homeland Security (DHS) Directive 110-01, Privacy Policy for Operational Use of Social Media.

II. Scope

This Instruction applies throughout DHS regarding the access to and collection, use, maintenance, retention, disclosure, deletion, and destruction of Personally Identifiable Information (PII) in relation to operational use of social media, with the exception of operational use of social media for: (a) communications and outreach with the public authorized by the Office of Public Affairs; (b) situational awareness by the National Operations Center; (c) situational awareness by Components other than the National Operations Center, upon approval by the Chief Privacy Officer following completion of a Social Media Operational Use Template; and (d) the conduct of authorized intelligence activities carried out by the Office of Intelligence and Analysis, the intelligence and counterintelligence elements of the United States Coast Guard, or any other Component performing authorized foreign intelligence or counterintelligence functions, in accordance with the provisions of Executive Order 12333, as amended. This Instruction does not apply to the Office of the Inspector General; however, the OIG will comply with the spirit of the Instruction.

III. References

A. Public Law 107-347, "E-Government Act of 2002," as amended, Section 208 [44 U.S.C. § 3501 note]

B. Title 5, United States Code (U.S.C.), Section 552a, "Records maintained on individuals" [The Privacy Act of 1974, as amended]

C. Title 6, U.S.C., Section 142, "Privacy officer"

D. Title 44, U.S.C., Chapter 35, Subchapter III, "Information Security" [The Federal Information Security Management Act of 2002, as amended (FISMA)]

E. Title 6, C.F.R., Chapter 1, Part 5, “Disclosure of records and information”

F. Directive 047-01, “Privacy Policy and Compliance”

G. DHS Sensitive Systems Policy Directive 4300A

H. Privacy-related memoranda issued by the Office of Management and Budget, including:

1. OMB Memorandum 10-22, “Guidance for Online Use of Web Measurement and Customization Technologies” (June 25, 2010)

2. OMB Memorandum 10-23, “Guidance for Agency Use of Third-Party Websites and Applications” (June 25, 2010)

3. OMB Memorandum 07-16, “Safeguarding Against and Responding to the Breach of Personally Identifiable Information" (May 22, 2007)

4. OMB Memorandum 06-20, “FY 2006 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management” (July 17, 2006)

5. OMB Memorandum 06-19, “Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments” (July 12, 2006)

6. OMB Memorandum 06-15, “Safeguarding Personally Identifiable Information” (May 22, 2006)

7. OMB Circular No. A-130, “Transmittal Memorandum #4, Management of Federal Information Resources” (November 28, 2000)

I. Privacy policy guidance and requirements issued (as updated) by the Chief Privacy Officer and published on the Privacy Office website, including:

1. Privacy Policy Guidance Memorandum 2008-02, *DHS Policy Regarding Privacy Impact Assessments* (December 30, 2008)

2. Privacy Policy Guidance Memorandum 2008-01, *The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security* (December 29, 2008)

3. Handbook for Safeguarding Sensitive Personally Identifiable Information at DHS (March 2012)

IV. Definitions

A. Counsel means the Office of the General Counsel attorney, from either the Immediate Office of the General Counsel or component counsel, assigned to provide legal advice to the component covered by this Instruction.

B. ***Fair Information Practice Principles*** means the policy framework adopted by the Department in Directive 047-01, Privacy Policy and Compliance, regarding the collection, use, maintenance, disclosure, deletion, or destruction of Personally Identifiable Information.

C. ***Individual*** means a natural person, including a United States citizen, Legal Permanent Resident, visitor to the United States, alien, DHS employee, or DHS contractor.

D. ***Operational Use*** means authorized use of social media to collect personally identifiable information for the purpose of enhancing situational awareness, investigating an individual in a criminal, civil, or administrative context, making a benefit determination about a person, making a personnel determination about a Department employee, making a suitability determination about a prospective Department employee, or for any other official Department purpose that has the potential to affect the rights, privileges, or benefits of an individual. Operational use does not include the use of search engines for general Internet research, nor does it include the use of social media for professional development such as training and continuing education or for facilitating internal meetings.

E. ***Personally Identifiable Information (PII)*** means any information that permits the identity of an individual to be directly or indirectly inferred, including other information that is linked or linkable to an individual.

For example, when linked or linkable to an individual, such information includes a name, Social Security number, date and place of birth, mother's maiden name, Alien Registration Number, account number, license number, vehicle identifier number, license plate number, device identifier or serial number, internet protocol address, biometric identifier (e.g., facial recognition photograph, fingerprint, iris scan, voice print), educational information, financial information, medical information, criminal or employment information, information created specifically to identify or authenticate an individual (e.g., a random generated number).

F. ***Privacy Compliance Documentation*** means any document required by statute or by the Chief Privacy Officer that supports compliance with DHS privacy policy, procedures, or requirements, including but not limited to the Social Media Operational Use Template (Template), Privacy Impact Assessments (PIAs), System of Records Notices (SORNs), Notices of Proposed Rulemaking for

Exemption from certain aspects of the Privacy Act (NPRM), and Final Rules for Exemption from certain aspects of the Privacy Act.

G. ***Privacy Compliance Review (PCR)*** means both the DHS Privacy Office process to be followed and the document designed to provide a constructive mechanism to improve a DHS program's ability to comply with assurances made in existing Privacy Compliance Documentation including Privacy Impact Assessments (PIAs), System of Records Notices (SORNs) and/or formal agreements such as Memoranda of Understanding or Memoranda of Agreement.

H. ***Privacy Impact Assessment (PIA)*** means both the DHS Privacy Office process to be followed and the document required whenever an information technology (IT) system, technology, rulemaking, program, pilot project, or other activity involves the planned use of PII or otherwise impacts the privacy of individuals as determined by the Chief Privacy Officer. A PIA describes what information DHS is collecting, why the information is being collected, how the information will be used, stored, and shared, how the information may be accessed, how the information will be protected from unauthorized use or disclosure, and how long it will be retained. A PIA also provides an analysis of the privacy considerations posed and the steps DHS has taken to mitigate any impact on privacy. As a general rule, PIAs are public documents. The Chief Privacy Officer may, in coordination with the affected component and the Office of the General Counsel, modify or waive publication for security reasons, or to protect classified, sensitive, or private information included in a PIA.

I. ***Program Manager*** means the DHS employee who is responsible for the planning and operation of a DHS program.

J. ***Situational Awareness*** means information gathered from a variety of sources that, when communicated to emergency managers and decision makers, can form the basis for incident management decision making.

K. ***Social Media*** means 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 take many different forms, including but not limited to web-based communities and hosted services, social networking sites, video and photo sharing sites, blogs, virtual worlds, social bookmarking, and other emerging technologies. This definition does not apply to internal Department intranets or applications.

L. ***Social Media Operational Use Template (Template)*** means the document that describes the current or proposed category of operational uses(s) of social media, identifies the appropriate authorities for the current or proposed category of use(s), describes what PII, if any, is collected (and from whom), and how that information is used. The Template is used to identify information technology systems, technologies, rulemakings, programs, or pilot projects that

involve collecting PII from social media for the proposed category of use(s) and to assess whether there is a need for additional Privacy Compliance Documentation. Templates are initially reviewed and adjudicated by the Chief Privacy Officer, and every three years thereafter for accuracy.

M. ***System Manager*** means the DHS employee identified in a System of Records Notice who is responsible for the operation and management of the system of records to which the System of Records Notice pertains.

N. ***System of Records Notice (SORN)*** means the official public notice of a DHS system of records as required by the Privacy Act of 1974 (as amended). The SORN identifies (1) the purpose for the system of records, (2) the individuals covered by information in the system of records, (3) the categories of records maintained about individuals, (4) the source of the records and (5) the ways in which the information is generally shared by the Department. The SORN also provides notice of the mechanisms available for individuals to exercise their Privacy Act rights to access and correct the PII that DHS maintains about them.

V. Responsibilities

A. ***All DHS employees*** are responsible for complying with Directive 110-01, with privacy policies and procedures issued by the Chief Privacy Officer, and with applicable Component policies on operational use of social media and for protecting PII from unauthorized use or disclosure.

B. ***Chief Information Officer*** is responsible for providing web technology services, security, and technical assistance for the operational use of social media within the Department.

C. ***Counsel*** is responsible for:

1. Providing advice to Program Managers or System Managers, as appropriate, to ensure that appropriate authority exists to engage in categories of operational use of social media before Component employees engage in those uses, and to ensure that the Template generally documents that authority; and

2. Providing legal guidance to the Component Privacy Officers or PPOCs and Program Managers or System Managers, as appropriate, in the drafting of Rules of Behavior for operational use of social media.

D. ***Component Privacy Officers*** are responsible for:

1. Maintaining an accurate accounting of all Component categories of operational use of social media using the Template to identify collection and use of PII, and any other attendant privacy impacts, and ensuring

Components implement DHS privacy policy with respect to the operational use of social media;

2. Coordinating with Program Managers or System Managers, as appropriate, together with the Chief Privacy Officer and counsel to complete a Template and any other required Privacy Compliance Documentation (1) for all proposed categories of operational use of social media, and (2) for any changes to the categories of operational use of social media;

3. Developing and reviewing Component policies and directives related to operational use of social media, and Component Rules of Behavior consistent with the adjudicated Template, to ensure compliance with DHS privacy policy, privacy laws applicable to DHS, and federal government-wide privacy policies;

4. Overseeing Component privacy training for operational use of social media and providing educational materials, consistent with privacy training for operational use of social media developed by the Chief Privacy Officer.

5. Reviewing documentation required in Section VI.D.8 to ascertain compliance with this Instruction as needed; and

6. Collaborating with the Chief Privacy Officer in conducting Privacy Compliance Reviews.

E. ***Privacy Points of Contact (PPOCs)*** are responsible for assuming the duties of Component Privacy Officers in Components that do not have Privacy Officers.

F. ***Program Managers*, or *System Managers, as appropriate,*** are responsible for:

1. Coordinating with the Component Privacy Officer or PPOC to ensure that privacy is appropriately addressed when proposing, developing, implementing, or changing any operational use of social media;

2. Coordinating with the Component Privacy Officer or PPOC and counsel to prepare drafts of the Template and, as appropriate, all Privacy Compliance Documentation required when proposing, developing, or implementing or changing any category of operational use of social media;

3. Monitoring the design, deployment, operation, and retirement of programs involving the operational use of social media to ensure that the

use of PII, if any, is limited to those uses described in the Privacy Compliance Documentation;

4. Ensuring oversight mechanisms are built into the design of programs and systems involving the operational use of social media;

5. Coordinating with the Component Privacy Officer or PPOC to establish administrative, technical, and physical controls for storing and safeguarding PII consistent with DHS privacy, security, and records management requirements to ensure the protection of PII from unauthorized access, disclosure, or destruction in the course of operational use of social media; and

6. Supporting the Component Privacy Officer or PPOC in developing and implementing privacy procedures and job-related privacy training to safeguard PII in operational uses of social media.

VI. Content and Procedures

A. Authority to Engage in Operational Use of Social Media: Program Managers and System Managers consult with counsel to ensure that appropriate authority exists to engage in categories of operational use of social media before Component employees engage in those activities.

B. Privacy Compliance Documentation: Before engaging in, or contracting for, new or modified categories of operational use of social media (which as defined includes investigatory purposes), Program Managers and System Managers, in consultation with Component Privacy Officers or PPOCs and counsel complete a Template to document the authority and purpose(s) of those uses as well as a description of those uses, and to determine whether all of the Rules of Behavior discussed in Section VI.D of this Instruction will apply to the particular uses(s) covered by the Template. Templates are submitted to the Chief Privacy Officer for a prompt review and determination as to whether a new or updated PIA or SORN is required. Templates are also completed to document categories of operational use of social media in existence prior to this Instruction to ensure compliance with this Instruction. Once a Template is approved for a category of operational use, a Template is not required for additional use of social media within that category unless there is a material modification of the Rules of Behavior applicable to that category. Components may appeal to the Deputy Secretary of Homeland Security if there is a disagreement over the DHS Privacy Office determination of privacy compliance for the operational use of social media.

C. Access: DHS employees who are granted access to use social media by their Component heads renew their access authority annually, consistent with

annual training requirements. Access is contingent upon an employee's successfully completing privacy training for operational use of social media.

D. Rules of Behavior: Component Privacy Officers or PPOCs, in coordination with counsel and Program Managers, or System Managers as appropriate, draft Rules of Behavior for operational use of social media (either separately or as part of a broader policy document) and submit them with the Template to the Chief Privacy Officer for review and approval. Personnel granted access to use social media certify annually that they have read and understand the Component Rules of Behavior. Where certification is not practicable, Component Privacy Officers and PPOCs maintain records of employee attendance at privacy training that includes training on Rules of Behavior.

Rules of Behavior include requirements for operational use of social media and the consequences of failure to adhere to those requirements. Where a federal policy establishes guidelines that apply to a Component's operational use of social media, the Component's Rules of Behavior incorporate that policy and that fact is noted in the Template. Unless otherwise noted in the Template adjudication process, the Rules of Behavior provide, at a minimum, that DHS employees:

1. Use social media for operational purposes only when activities are authorized by statute, executive order, regulation, or policy;

2. Use only government-issued equipment, government accounts, and only government email addresses when engaging in the operational use of social media;

3. Use online screen names or identities that indicate an official DHS affiliation and use DHS email addresses to open accounts used when engaging in social media in the performance of their duties;

4. Access publicly available information through social media only by reviewing posted information without interacting with any individual who posted the information;

5. Respect individuals' privacy settings and access only information that is publicly available unless the individual whose information the employee seeks to access has given consent to access it;

6. Collect the minimum PII necessary for the proper performance of their authorized duties;

7. Protect PII as required by the Privacy Act and DHS privacy policy; and

8. Document operational use of social media, including date, site(s) accessed, information collected, and how it was used in the same manner that the Department would document information collected from any source in the normal course of business. For instance, where information obtained through authorized operational use of social media is used in whole or in part to make decisions regarding an individual's rights, benefits or privileges, employees document that fact in relevant records.

E. Privacy Training: Component Privacy Officers or PPOCs tailor privacy training for the operational use of social media to Component-specific needs, based upon training materials provided by the Chief Privacy Officer. Completion of this privacy training is a prerequisite for obtaining access to social media for operational use. Upon completion of this training, employees will certify that they have read and understand their Component's Rules of Behavior. Where certification is not practicable, Component Privacy Officers and PPOCs maintain records of employee attendance at privacy training that includes training on Rules of Behavior. Employees also complete refresher training and recertify they have read and understand their Component's Rules of Behavior annually thereafter. Privacy training content includes, at a minimum, legal authorities, acceptable operational uses of social media, access requirements, applicable Rules of Behavior, and requirements for documenting operational uses of social media.

F. Retention of PII: Component Program Managers or System Managers where appropriate, maintain PII collected through authorized operational uses of social media in the applicable Privacy Act system of records in accordance with approved records retention schedules.

G. Privacy Compliance Reviews (PCR): The Chief Privacy Officer, in collaboration with Component Privacy Officers or PPOCs, conducts PCRs of approved operational uses of social media periodically, at the sole discretion of the Chief Privacy Officer, to ascertain compliance with DHS privacy policy and legal authorities. PCRs may include a determination as to whether the Privacy Compliance Documentation for a particular operational use of social media is accurate and up to date.

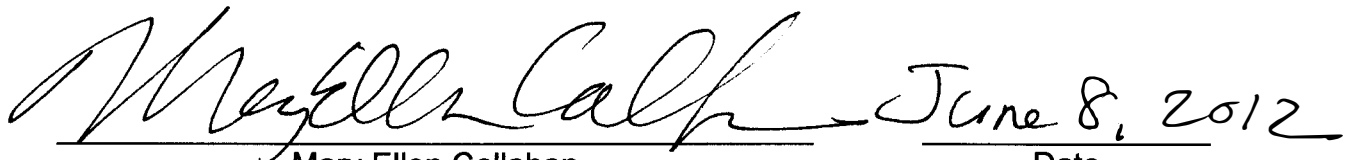
H. Implementation: Measured from the date Directive 110-01 and this Instruction are signed and posted on DHS Connect:

1. the Chief Privacy Officer provides baseline training to the Components within 45 days, and

2. Components complete implementation of this Instruction, including obtaining approval from the Chief Privacy Officer of Templates for categories of operational use of social media in existence prior to this Instruction, within 120 days, except that Components complete training of all pertinent employees within 165 days.

VII. Questions

Address any questions or concerns regarding these Instructions to the DHS Privacy Office or to the relevant Component Privacy Officer or PPOC.



June 8, 2012

Mary Ellen Callahan
Chief Privacy Officer

Date