The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
202-343-1717, pia@dhs.gov
www.dhs.gov/privacy

DHS OPERATIONAL USE OF SOCIAL MEDIA

This template is used to assess the Department's Operational Use of Social Media, consistent with Management Directive 110-01.

The DHS Privacy Office has created this template to determine privacy compliance with Management Directive 110-01, *Privacy Policy for Operational Use of Social Media*. For the purposes of the Management Directive and this template, "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. The following uses of social media are exempt from the Management Directive and are not subject to this requirement[1]:

a) Communications and outreach with the public authorized by the Office of Public Affairs (covered by the existing PIAs: DHS/ALL/PIA-031 - Use of Social Networking Interactions and Applications Communications/Outreach/Public Dialogue and DHS/ALL/PIA-036 - Use of Unidirectional Social Media Applications);

b) 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 template shall be used to document the process to be followed by all programs engaging in operational uses of social media; to identify information technology systems, technologies, rulemakings, programs, or pilot projects that involve PII and other activities that otherwise impact the privacy of individuals as determined by the Chief Privacy Officer; and to assess whether there is a need for additional Privacy Compliance Documentation. Components may appeal to the Deputy Secretary for Homeland Security if there is disagreement over the DHS Privacy Office determination of privacy compliance for the operational use of social media.

[1] Gathering information by the Office of Operations Coordination and Planning (OPS) to enhance situational awareness is exempt from this requirement and is covered by the existing PIA: DHS/OPS/PIA-004(d) - Publicly Available Social Media Monitoring and Situational Awareness Initiative Update.

DHS OPERATIONAL USE OF SOCIAL MEDIA

Please complete this form and send it to your Component Privacy Officer. Upon receipt, your Component Privacy Officer and the DHS Privacy Office will review this form and may request additional information.

SUMMARY INFORMATION

Date submitted for review: January 12, 2017

Name of Component: Office of Security

Contact Information: (b)(6) **or** (b)(6)
(b)(6)

Counsel[2] Contact Information: Logan Perel, (b)(6)

IT System(s) where social media data is stored: C-LAN Insider Threat Enclave known as FENCE (Filtered Enhanced Network Containment Enclave)

Applicable Privacy Impact Assessment(s) (PIA): DHS Insider Threat Program, DHS/ALL/PIA-052 dated 7/13/2015

Applicable System of Records Notice(s) (SORN): Department of Homeland Security/ALL–038 Insider Threat Program System of Records

[2] Counsel listed here must certify that appropriate authority exists to engage in particular operational activities involving social media.

DHS OPERATIONAL USE OF SOCIAL MEDIA

SPECIFIC QUESTIONS

1. **Describe the category of use for collecting personally identifiable information from social media sources. Examples include: law enforcement intelligence, criminal investigations, background investigations, administrative investigations, professional responsibility investigations, benefit or employment determinations, or situational awareness. If use does not fit into one of these categories, please describe in full below. If your component has multiple categories of use, please submit separate template for each category.**

   Publicly available social media will be collected in support of open Insider Threat inquiries that are performed in accordance with the ITOC (Insider Threat Operations Center) SOP dated 7/10/15, which was previously approved by OGC, PRIV, and CRCL. Furthermore, all inquirers are reported quarterly to the Insider Threat Oversight Group (OGC, PRIV, and CRCL).

2. **Based on the operational use of social media listed above, please provide the appropriate authorities.**

   - Executive Order 13587 - Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information
   - Presidential Memorandum - National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs
   - DHS Delegation of Authority 08503 (Aug. 10, 2012)
   - DHS Directive 262-05, Information Sharing and Safeguarding (Sept. 4, 2014)
   - DHS Instruction 262-05-01, Insider Threat Program (July 9, 2015)
   - DHS Delegation 12000, Chief Security Officer (June 5, 2012)
   - Title 6 U.S.C. § 341(a)(6), Under Secretary for Management

   a) **Has Counsel listed above reviewed these authorities for privacy issues and determined that they permit the Program to use social media for the listed operational use?**

   ☒ Yes. ☐ No.

3. **Is this use of social media in development or operational?**

   ☐ In development. ☒ Operational. Date first launched:

4. **Please attach a copy of the Rules of Behavior that outline the requirements below.**

   See attached.

5. Please describe the Rules of Behavior in effect for the listed operational use of social media. If users do NOT follow a particular Rule, please detail reasoning for not following that Rule:

a) *Equipment*. Use only government-issued equipment when engaging in the operational use of social media;

☒ Yes. ☐ No. If not, please explain:

b) *Email and accounts*. 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;

☐ Yes. ☒ No. If not, please explain: To the extent the ITOC collects publicly available information, this may be done by accounts that are not registered to DHS, however, only publicly available information will be collected.

c) *Public interaction*. Access publicly available information through social media only by reviewing posted information without interacting with any individual who posted the information;

☒ Yes. ☐ No. If not, please explain:

d) *Privacy settings*. Respect individuals' privacy settings and access only information that is publicly available;

☒ Yes. ☐ No. If not, please explain:

e) *PII collection*: Collect the minimum PII necessary for the proper performance of their authorized duties except for systems subject to Final Rules for Exemption from certain aspects of the Privacy Act;

☒ Yes. ☐ No. If not, please explain:

f) *PII safeguards*. Protect PII as required by the Privacy Act (if applicable) and DHS privacy policy;

☒ Yes. ☐ No. If not, please explain:

g) *Documentation*. Document operational use of social media, including date, site(s) accessed, information collected and how it was used in the same manner as the component would document information collected from any source in the normal course of business.

☒ Yes. ☐ No. If not, please explain:

h) *Training*. Users complete annual privacy training which has been approved by Component Privacy Officer (or Privacy Point of Contact) based upon training materials provided by the DHS Privacy Office. Training must include, at minimum: legal authorities, acceptable operational uses of social media, access requirements, and requirements for documenting operational uses of social media.

☒ Yes. ☐ No. If not, please explain:

Mechanisms are (or will be) in place to verify that users have completed training.

☒ Yes, employees self-certify that they have read and understood their Component Rules of Behavior.

☒ Yes, Component Privacy Officers or PPOCs maintain a record of employee attendance at privacy training that includes training on the Rules of Behavior.

☐ No. If not, please explain:

DHS SOCIAL MEDIA DOCUMENTATION

(To be Completed by the DHS Privacy Office)

DATE reviewed by the DHS Privacy Office: 1/12/17

NAME of the DHS Privacy Office Reviewer: (b)(6)

DHS Privacy Office Determination

☒ Program has met requirements to use social media for the stated authorized operational purposes, and must continue compliance with the requirements above.

☐ Program has not yet met requirements to utilize social media for operational purposes.

☐ Program authorities do not authorize operational use of social media.

☐ Rules of Behavior do not comply. <Please explain analysis.>

☐ Training required.

Additional Privacy compliance documentation is required:

☒ A PIA is required.

☒ Covered by existing PIA. DHS/ALL/PIA-052 DHS Insider Threat Program

☐ New.

☐ Updated. <Please include the name and number of PIA to be updated here.>

☒ A SORN is required:

☒ Covered by existing SORN. DHS/ALL-038 Insider Threat Program System of Records, February 26, 2016, 81 FR 9871

☐ New.

☐ Updated. <Please include the name and number of SORN to be updated here.>

DHS PRIVACY OFFICE COMMENTS

The DHS Privacy Office finds that the Insider Threat Program's use of Social Media is consistent with existing privacy compliance documentation. The Insider Threat Program has the authority to collect social media information from postings that are

publicly available in support of open insider threat inquiries. This information collection will involve only passively viewing user information, and program personnel may not interact with users online as part of this effort.

The DHS Privacy Office finds that PIA coverage for this effort is provided by DHS/ALL/PIA-052 DHS Insider Threat Program, which describes the Insider Threat Program's access to, and collection of information, including PII, associated with: DHS personnel who possess security clearances; state, local, tribal, territorial, and private sector individuals who possess security clearances granted by DHS; and any other individual who possesses a security clearance and accesses DHS IT systems or DHS classified information. SORN coverage is provided by DHS/ALL-038 Insider Threat Program System of Records, which outlines the collection and maintenance of records to manage insider threat matters; facilitate insider threat investigations and activities associated with counterintelligence and counterespionage complaints, inquiries, and investigations; identify threats to DHS resources and information assets; track referrals of potential insider threats to internal and external partners; and provide statistical reports and meet other insider threat reporting requirements.