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:

Name of Component: U.S. Customs and Border Protection

Contact Information: (b) (6), (b) (7)(C) **Director, Personnel Security Division** (b) (6), (b) (7)(C) (b) (6), (b) (7)(C)

Counsel[2] Contact Information: (b) (6), (b) (7)(C) **Associate Chief Counsel, Ethics, Labor & Employment**

IT System(s) where social media data is stored:

- Integrated Security Management System (ISMS)

Applicable Privacy Impact Assessment(s) (PIA):

- DHS/ALL/PIA-038(c) Integrated Security Management System (ISMS), June 26, 2017
- Forthcoming Background Investigations PIA

Applicable System of Records Notice(s) (SORN):

- DHS/ALL-023 - Department of Homeland Security Personnel Security Management, February 23, 2010, 75 FR 8088

[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.**

   This SMOUT addresses the operational use of social media during background investigations and adjudications for determining initial or continued suitability for employment, eligibility to occupy a national security position, eligibility for access to classified information, eligibility for unescorted access to DHS/CBP facilities, or access to DHS/CBP information technology systems. The personnel using social media under this SMOUT are Office of Professional Responsibility (OPR), Personnel Security Division (PSD), employees and persons contracted by OPR PSD to support the background investigation, periodic reinvestigation, and continuous evaluation process.

   This SMOUT encompasses both (b) (7)(E)

   (b) (7)(E)

   (b) (7)(E)

   (b) (7)(E)

   (b) (7)(E)

   (b) (7)(E)

   In addition to sharing information with OPR IOD, OPR PSD may also share information with other entities as required by regulation.

   (b) (7)(E)

(b) (7)(E)

(b) (7)(E) will be stored in the Integrated Security Management System (ISMS), which is covered under the DHS/ALL-023 Department of Homeland Security Personnel Security Management SORN. OPR PSD is not involved in the gratuitous gathering of personal social media information or PII. In addition, OPR does not collect or store as evidence any social media information that is solely an exercise of rights protected by the First Amendment (b) (7)(E)

(b) (7)(E)

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

- Executive Order (E.O.) 10450; E.O. 12968; E.O. 13467; E.O. 13488; E.O. 13764
- 5 CFR Parts 731, 732, 736, and 1400; 32 CFR Part 147
- Security Executive Agent Directive 4, National Security Adjudicative Guidelines
- Security Executive Agent Directive 5, Collection, Use, and Retention of Publicly Available Social Media Information in Personnel Security Background Investigations and Adjudications
- Director of Central Intelligence Directive 6/4
- DHS Delegation No. 12000, Delegation for Security Operations Within the Department of Homeland Security
- DHS Directive 110-01, Privacy Policy for Operational Use of Social Media (June 8, 2012), and Instruction 110-01-001, Privacy Policy for Operational Use of Social Media (June 8, 2012).
- CBP Directive No. 2130-016, Roles and Responsibilities for Internal Affairs Activities and Functions (December 23, 2008)
- CBP Directive No. 5410-003, Operational Use of Social Media (January 2, 2015)

(b) (5)

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

☒ In development. ☐ Operational.

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

Attached. Also attached is the CBP Directive for Operational Use of Social Media.

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:**

(b) (7)(E)

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;

(b) (7)(E) [redacted]

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

d) (b) (7)(E) [redacted] *Privacy settings*. Respect individuals' privacy settings and access only information that is publicly available;

(b) (7)(E) [redacted]

e) *PII collection*: Collect the minimum PII necessary for the proper performance of 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.

☒ 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: 5/16/2018**

NAME **of** the DHS Privacy Office Reviewer: (b) (6), (b) (7)(C)

DESIGNATION

This program is covered by the following Privacy Impact Assessment and Privacy Act System of Records Notice:

PIA: New CBP Background Investigations PIA

SORN: Update to DHS/ALL-023 Department of Homeland Security Personnel Security Management, February 23, 2010, 75 FR 8088

1. **Category of Use:**

☐ Law Enforcement Intelligence;

☐ Criminal law enforcement investigations;

☒ Background investigations;

☒ Professional responsibility investigations;

☐ Administrative or benefit determinations (including fraud detection);

☐ Situational awareness; and

☐ Other. <Please explain "other" category of use here.>

(b) (5)

3. **Rules of Behavior Content: (Check all items that apply.)**

a. *Equipment.*

(b) (7)(E)

b. *Email and accounts*.

(b) (7)(E) [redacted]

c. *Public interaction*.

(b) (7)(E) [redacted]

d. *Privacy settings*.

☐ Users may disregard privacy settings.

☒ Users must respect individual privacy settings.

e. *PII storage*:

☐ PII is maintained in an exempted Privacy Act System of Records.

Please list applicable SORN here:

☒ PII is maintained in a Privacy Act Systems of Records.

Please list applicable SORN here: DHS/ALL-023 Department of Homeland Security Personnel Security Management, February 23, 2010, 75 FR 8088 - SORN must be updated with social media information as a Category of Record.

f. *PII safeguards*.

☒ PII is protected as required by the Privacy Act and DHS privacy policy.

☐ Only a minimal amount of PII is collected and safeguarded, consistent with DHS/OPS-004 – Publicly Available Social Media Monitoring and Situational Awareness Initiative.

g. *Documentation*.

☒ Users must appropriately document their use of social media, and collection of information from social media website.

☐ Documentation is not expressly required.

h. *Training*.

☒ All users must complete annual privacy training that has been approved by Component Privacy Officer. Training includes:

☒ Legal authorities;

☒ Acceptable operational uses of social media;

☒ Access requirements;

☒ Applicable Rules of Behavior; and

☒ Requirements for documenting operational uses of social media.

☒ 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, certification of training completion cannot be verified.

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.

☒ New. CBP Background Investigations PIA

☐ Updated.

☒A SORN is required:

☐ New.

☒ Updated. DHS/ALL-023 Department of Homeland Security Personnel Security Management, February 23, 2010, 75 FR 8088

DHS PRIVACY OFFICE COMMENTS

CBP Privacy is submitting this SMOUT to discuss the operational use of social media during background investigations and adjudications for determining initial or continued suitability for employment, eligibility to occupy a national security position, eligibility for access to classified information, eligibility for unescorted access to DHS/CBP facilities, or access to DHS/CBP information technology systems.

The personnel using social media under this SMOUT are Office of Professional Responsibility (OPR), Personnel Security Division (PSD), employees and persons contracted by OPR PSD to support the background investigation, periodic reinvestigation, and continuous evaluation process.

This SMOUT encompasses both (b) (7)(E), (b) (5) OPR PSD's use of social media for (b) (7)(E), (b) (5)

(b) (7)(E), (b) (5)

OPR PSD will use the (b) (7)(E), (b) (5)

(b) (7)(E), (b) (5)

The DHS Privacy Office finds that CBP's operational use of social media by OPR PSD is consistent with its background investigation responsibilities and authorities.

A new CBP Background Investigations PIA will be required to discuss the collection of social media information by OPR PSD to support the background investigation, periodic reinvestigation, and continuous evaluation process. SORN coverage is provided by the DHS/ALL-023 Department of Homeland Security Personnel Security Management SORN, which will need to be updated to include social media information as a Category of Records.