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: 09/18/2015

Name of Component: Customs and Border Protection

Contact Information: (b) (6), (b) (7)(C)

Counsel[2] Contact Information: Marc Bennett Courey, Office of Chief Counsel, Enforcement Section

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

- Joint Integrity Case Management System (JICMS),
- Integrated Security Management System (ISMS).

Applicable Privacy Impact Assessment(s) (PIA):

- DHS/ALL/PIA-038(a), Integrated Security Management System Update September 16, 2014,
- JICMS PIA is currently being drafted

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

- DHS/ALL-020 - Department of Homeland Security Internal Affairs April 28, 2014, 79 FR 23361

[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.**

The personnel anticipated to use social media under this SMOUT are Office of Internal Affairs Investigative Operations Division and Credibility Assessment Division personnel. This SMOUT encompasses using (b) (7)(E) (b) (7)(E) All allegations against CBP employees are entered through the Joint Intake Center (JIC) process. The CBP Office of Internal Affairs (IA) JIC and Investigative Operations Division (IOD) vets those allegations to determine whether any allegation of corruption and other misconduct rise to the level of criminal conduct. For those allegations determined by Management to be criminal in nature, IA requires the use of (b) (7)(E) (b) (7)(E) (some of which may be Personally Identifiable Information (PII), per DHS Instruction 110-01-001, Section IV E), in publicly accessible/non-privacy restricted social media forums. This publically accessible/non-privacy restricted information has the potential to (b) (7)(E) (b) (7)(E)

CBP IA will use social media to (b) (7)(E) (b) (7)(E) IA will not be involved in the gratuitous gathering of personal social media information or PII. IA does not collect or store as evidence any social media information that is solely an exercise of political speech. IA's focus is solely on identifying information that is (b) (7)(E) (b) (7)(E)

Once an individual is the subject of a criminal investigation, IA will use social media to (b) (7)(E) (b) (7)(E) The information is stored in the Joint Integrity Case Management System is the IT system, which is covered under the DHS/ALL-20- Internal Affairs SORN.

(Note: While some IA investigations are clearly administrative, based on a lack of correlation between activity and criminal statutes, some criminal investigations may become administrative in nature. Once a competent prosecuting authority (i.e., the US Attorney's Office) declines prosecution of an investigation, it may become an administrative matter. This change in the character of the investigation is a function of prosecutorial discretion, and not an arbitrary decision on the part of IA. Once prosecution of the matter is declined, IA will conduct any further investigation of the matter pursuant to the Internal Affairs Non-Criminal Investigation SMOUT.

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

Authorities to conduct [redacted] for criminal investigations includes Title 19 of the U.S. Code, including but not limited to 19 U.S.C. §§ 1589a and 2081, 8 U.S.C. § 1363a (criminal investigations for immigration violations) and by virtue of the Commissioner's Delegation Order (Customs Order No. 09-007), Section 287 of the Immigration and Nationality Act and its implementing regulations regarding enforcement authorities and responsibilities. See 8 CFR 287.2 (initiating criminal investigation for immigration violations); 8 CFR 287.4 (issue subpoenas in criminal or civil investigations); 8 CFR 287.9 (obtaining search warrant prior to conducting a search in a criminal investigation). Additionally, as of September 18, 2014, the Secretary delegated authority to CBP IA to investigate its employees for alleged criminal misconduct. See also CBP Directive No. 2130-016, "Roles and Responsibilities for Internal Affairs Activities and Functions" (December 23, 2008) and CBP Delegation Order 09-007 "Authority to Designate Federal, State, Local, Tribal and Foreign Law Enforcement Officers as "Customs Officers"; Customs Officer Authority, Immigration Officer Authority (December 21, 2009).

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: 10/1/2004

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, Section 5

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:

When IA investigators are conducting a criminal investigation, they may (as is common law enforcement practice in analogous situations) (b) (7)(E) (b) (7)(E) This being said, the viewing of publically available information/non-privacy restricted social media information may require no interaction with the individual under investigation, so the

(b) (7)(E)

Yes- When CBP uses (b) (7)(E) CBP personnel do not log in, so no profile is created.

No- When Office of Internal Affairs Investigative Operations Division and Credibility Assessment Division personnel conduct limited (b) (7)(E) on social media sites, they need to (b) (7)(E) .

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.

☒ 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: January 28, 2016

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

DESIGNATION

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.
- ☒ Incomplete privacy compliance documentation.

Additional Privacy compliance documentation is required:

- ☒ A PIA is required.
  - ☒ New.
  - ☐ Updated. <Please include the name and number of PIA to be updated here.>
- ☒ A SORN is required:
  - ☐ New.
  - ☒ Updated. DHS/ALL-020 - Department of Homeland Security Internal Affairs April 28, 2014, 79 FR 23361

DHS PRIVACY OFFICE COMMENTS

The DHS Privacy Office finds that CBP's operational use of social media for internal affairs criminal investigations purposes is consistent with their internal affairs investigatory authorities. CBP Internal Affairs has authority to conduct investigations using open source, publicly available information from social media as they would any other type of publicly available information collection. We also agree that due to the nature of their investigatory needs, they may (b) (7)(E) (b) (7)(E) CBP IA must still follow all other standard rules of behavior.

However, the DHS Privacy Office also finds that the compliance documentation for this program is incomplete and requires an immediate update. CBP must complete the (b) (5) [redacted]. In addition, DHS will update the DHS/ALL-020 Internal Affairs SORN to more clearly represent open source social media as a category of records and record source.

These outstanding compliance requirements must be completed within six months (July 28, 2016).

PCTS # 1112054.