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: 07/19/2017

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

Contact Information: (b) (6), (b) (7)(C) Senior Special Agent, (b) (6), (b) (7)(C)

Counsel[2] Contact Information: (b) (6), (b) (7)(C) Associate Chief Counsel, Enforcement and Operations

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

- Joint Integrity Case Management System (JICMS),

Applicable Privacy Impact Assessment(s) (PIA):

- DHS/CBP/PIA-044, Joint Integrity Case Management System (JICMS), July 18, 2017

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.**

This SMOUT addresses the operational use of social media for administrative investigations in a professional responsibility context. The personnel anticipated to use social media under this SMOUT are assigned to the Office of Professional Responsibility (OPR) Investigative Operations Division (IOD). All allegations against CBP employees are entered through the Joint Intake Center (JIC) process. The CBP OPR JIC and IOD vet the allegations to determine whether any allegation of corruption or misconduct rise to the level of criminal activity. If an allegation is determined to rise to the level of criminal activity, the investigation will proceed under the CBP OPR SMOUT for criminal investigations. If an allegation does not rise to the level of criminal activity, or if a prosecutor determines that a case cannot viably be criminally prosecuted, then OPR IOD will treat it as an administrative investigation. OPR IOD conducts administrative investigations for employee misconduct (improper fraternization, neglect of duty, mismanagement, etc.) in order to ensure compliance with CBP rules and prevent against corruption. In the process of these investigations OPR IOD will use the internet, including social media, to investigate, gather evidence, and gather information on activities by CBP employees or contractors that is pertinent to allegations of misconduct by an employee or contractor. (b) (7) (E) [redacted]

OPR IOD will not be involved in the gratuitous gathering of personal social media information or PII. OPR IOD's focus is solely on identifying information that is germane to either proving or disproving allegations of misconduct. All OPR IOD investigations are predicated on specific allegations or articulable facts that are prima facie indicators of misconduct.

Once an individual is the subject of an investigation, OPR IOD will use the Internet, including social media as defined in DHS Instruction 110-01-001, Privacy Policy for the Operational Use of Social Media (Privacy Policy), for administrative investigations in a professional responsibility context that do not rise to the level of criminal misconduct or where prosecution is declined to gather evidence and relevant information related to misconduct. (b) (7)(E) [redacted] (b) (7)(E) [redacted] The information is stored in the Joint Integrity Case Management System (JICMS), which is covered under the DHS/ALL-20- Internal Affairs SORN and the JICMS PIA.

This use of the Internet, including social media, involves activities to gather information pertinent to allegations of misconduct by an employee or contractor, such as (b) (7)(E) [redacted] (b) (7)(E) This information is gathered and used by CBP OPR IOD personnel in the same manner as information gathered from non-Internet and non-social media sources such as information gathered in person, on the phone, or through

research of hard copy documents. Information gathered in this fashion may be used in administrative investigations of employees or contractors of CBP.

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

- Homeland Security Act of 2002 § 411(c) & (j), Pub. L. No. 107-296, 116 Stat. 2135 (2002) as amended by section 802 of the Trade Enforcement and Trade Facilitation Act of 2015, Pub. L. No. 114-25 (2016) (codified at 6 U.S.C. § 211(c) & (j))
- Inspector General Act of 1978, Pub. L. 95–452, 92 Stat. 1101 (1978), as amended (codified at 5 U.S.C. App.)
- DHS Delegation No. 7010.3, Delegation of Authority to the Commissioner of U.S. Customs and Border Protection
- DHS Management Directive 0810.1, The Office of Inspector General
- CBP Directive No. 2130-016, Roles and Responsibilities for Internal Affairs Activities and Functions (December 23, 2008)

(b) (5)

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

☐ In development. ☒ Operational. Date first launched: July 18, 2017

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;

(b) (7)(E)

(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;

(b) (7)(E)

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

(b) (7)(E)

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:

H
S

DHS SOCIAL MEDIA DOCUMENTATION

(To be Completed by the DHS Privacy Office)

DATE reviewed by the DHS Privacy Office: 2/12/2018

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: DHS/CBP/PIA-044 Joint Integrity Case Management System (JICMS)

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

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) Users must use government-issued equipment. Equipment may be non-attributable and may not resolve back to DHS/US IP address.

(b) (7)(E) Users must use government-issued equipment. Equipment must resolve back to DHS/US IP address.

b. *Email and accounts*.

(b) (7)(E) Users do not have to use government email addresses or official DHS accounts online.

(b) (7)(E) sers must use government email addresses or official DHS accounts online.

c. *Public interaction*.

(b) (7)(E) Users may interact with individuals online in relation to a specific law enforcement investigation.

(b) (7)(E) Users may NOT interact with individuals online.

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

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

Please list applicable SORN here:

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.

☒ Covered by existing PIA. DHS/CBP/PIA-044 Joint Integrity Case Management System (JICMS)

☐ New.

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

☒ A SORN is required:

☒ Covered by existing SORN. DHS/ALL-020 Department of Homeland Security Internal Affairs, April 28, 2014, 79 FR 23361

☐ New.

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

DHS PRIVACY OFFICE COMMENTS

CBP is submitting this SMOUT to discuss the operational use of social media for administrative investigations in a professional responsibility context. Office of Professional Responsibility (OPR) Investigative Operations Division (IOD) personnel will use social media to investigate allegations against CBP employees to vet the allegations to determine whether any allegation of corruption or misconduct rise to the level of criminal activity. If an allegation does not rise to the level of criminal activity, or if a prosecutor determines that a case cannot viably be criminally prosecuted, then OPR IOD will treat it as an administrative investigation. OPR IOD conducts administrative investigations for employee misconduct (improper fraternization, neglect of duty, mismanagement, etc.) in order to ensure compliance with CBP rules and prevent against corruption.

CBP OPR IOD will use social media to gather evidence directly relevant to the activity that predicates its investigation. OPR IOD will not gather PII that is not relevant to the investigation pursuant to OPR IOD investigation training standards and guidelines, the CBP Directive for Operational Use of Social Media, the CBP Rules of Behavior, and the DHS Privacy Policy for the Operational Use of Social Media. OPR IOD's focus is solely on identifying information that is germane to either proving or disproving allegations of administrative violations or misconduct. (b) (7)(E) [redacted] (b) (7)(E) [redacted] The information is stored in the Joint Integrity Case Management System (JICMS).

While some investigations are clearly administrative, some criminal investigations may become administrative in nature. Once a prosecuting authority 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 OPR.

The DHS Privacy Office finds that CBP's operational use of social media for internal affairs administrative investigations purposes is consistent with their internal affairs investigatory authorities. PIA coverage is provided by DHS/CBP/PIA-044 Joint Integrity Case Management System (JICMS). SORN coverage is provided by DHS/ALL-020 Department of Homeland Security Internal Affairs.