The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
202-(b) (7)(E)@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: 1/2/19

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

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

Counsel[2] Contact Information: (b) (6), (b) (7)(C) **Deputy Associate Chief Counsel, Enforcement & Operations, Office of Chief Counsel, U.S. Customs and Border Protection,** (b) (6), (b) (7)(C) (b) (6), (b) (7)(C) **(Main)**

IT System(s) where social media data is stored: The information may be stored on CBP SharePoint sites, CBP workstations, or in DHS electronic mail.

Applicable Privacy Impact Assessment(s) (PIA):

- **The CBP Privacy Office finds that overarching PIA coverage for this effort is provided by:**
  - **DHS/ALL/PIA-056 DHS and Component Network IT Security Operations and Privacy and IT Security Incident Response, which outlines the Department's efforts to protect the confidentiality, integrity, and availability of DHS information and information assets.**
    - **Coverage under this PIA includes situations where CBP OIT identifies an issue of concern on Social Media in which the PII of the individual that posted it is not relevant or necessary. In those instances, CBP OIT would redact PII from any notifications or work products that are produced or stored.**
  - **DHS/CBP/PIA-010(a) Analytical Framework for Intelligence, which outlines CBP's efforts to identify, apprehend, and prosecute individuals who pose a potential law enforcement or security risk, and aids in the enforcement of customs, immigration, and other laws enforced by DHS.**
    - **Coverage under this PIA includes situations where CBP OIT identifies a social media post in which a cyber-threat actor indicates an intent to conduct an attack on or hack of CBP. In these instances, the PII of the**

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

individual that created the post is relevant and would be included in notifications and work products, and would be retained in AFI.

- **The CBP Privacy Office is working with the Department and other Components to develop more specific coverage in the future, however DHS/ALL/PIA-056 and DHS/CBP/PIA-010(a) cover all aspects of this effort, including the collection and use of social media.**

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

The CBP Privacy Office finds that SORN coverage for this effort is provided by DHS/CBP-024 Intelligence Records System (CIRS) System of Records, September 21, 2017, 82 FR 44198, which describes CBP's collection, maintenance, and use of records in order to identify, apprehend, or prosecute individuals who pose a potential law enforcement or security risk; aid in the enforcement of the customs and immigration laws, and other laws enforced by DHS at the border; and enhance U.S. border security.

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 in support of the protection and cybersecurity of CBP information systems and networks. The personnel using social media under this SMOUT are Cyber Threat Analysts employed in CBP's Cyber Threat Intelligence (CTI) team in the Office of Information and Technology (OIT), Cybersecurity Directorate, Security Operations Division. (b) (7)(E)

(b) (7)(E)

CTI's mission statement is to "enhance the cybersecurity posture of CBP information systems and networks through the aggregation, correlation, and dissemination of intelligence and information on cyberspace threats."

- **Aggregation and Correlation**: The primary role of the operational use of social media is to enable CTI team to identify and collect information on cyberspace threats either currently impacting CBP's information technology environment or with the potential to impact that environment. When a threat is identified, the CTI team

(b) (7)(E)

- In some cases, the CTI team will receive information from the CBP Security Operations Center that CBP was affected by specific cyber threat activity (e.g., phishing emails targeting CBP employees, malware on employee workstations, reconnaissance activities against CBP's network). In other cases, the CTI team will receive or identify a report, article, blog, or other open source information suggesting that a cyber-threat actor is conducting malicious activity against U.S. Government or

other relevant entity. And in other cases, the CTI team will receive an alert related to a suspicious website related to CBP that warrants further investigation using a secured Internet browsing capability. Regardless of the situation, the CTI team will

(b) (7)(E)

NOTE: The sole purpose of the CTI team maintaining access to social media is to view the publicly-available posts in the event that such posts contain information related to cyber threat activity; not to engage with individuals on social media. In addition, (b) (7)(E)

(b) (7)(E)

- **Storage**: Once the CTI team identifies specific information of interest, the team will typically either save a screenshot of the resulting website or create a PDF copy of the resulting website, including social media posts. Typically, CTI will save the file to their workstation and upload the file to an internal, restricted-access SharePoint website on CBPNet that contains CTI's investigation information. The information posted on the website is restricted to personnel within the Cybersecurity Directorate with a need-to-know (i.e., the CTI team, CBP Security Operations Center personnel, Security Operations Division leadership, and the Chief Information Security Officer). The purpose of uploading this information to the site is to ensure that it is available to all CTI and other cybersecurity analysts during ongoing investigation activities. In addition, the site also provides a historical record in the event that the CTI team must conduct retroactive analysis of the related investigation. The information is stored subject to the applicable records retention policies.

Dissemination: **Other than the SharePoint site, the dissemination of information gathered will almost always be limited to email communications. The vast majority of information gathered and shared is between the CTI team and the CBP Security Operations Center personnel. It is also possible that the CTI team would share information outside of CBP or DHS, such as the FBI or other U.S. Government**

Departments or Agencies with cyber threat intelligence and/or cybersecurity missions. The CTI team will be required to mark the information with proper handling instructions before sharing, whether inside or outside of DHS. The CTI team understands the need-to-know concept, and ensures that operational information related to ongoing investigations is retained for the duration of that investigation.

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

- Homeland Security Act of 2002, as amended, 6 U.S.C. § 101, et seq.
- Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. § 3551, et seq.
- 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. 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. Date first launched:

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

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)

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 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: 04/26/2019

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

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-056 DHS and Component Network IT Security Operations and Privacy and IT Security Incident Response; DHS/CBP/PIA-010(a) Analytical Framework for Intelligence
  - ☐ New.
  - ☐ Updated. <Please include the name and number of PIA to be updated here.>
- ☒ A SORN is required:
  - ☒ Covered by existing SORN. DHS/CBP/PIA-010(a) Analytical Framework for Intelligence
  - ☐ New.
  - ☐ Updated. <Please include the name and number of SORN to be updated here.>

DHS PRIVACY OFFICE COMMENTS

CBP is submitting this PTA to discuss OIT use of social media in support of protection and cybersecurity of CBP information systems and networks. (b) (7)(E)
(b) (7)(E)
(b) (7)(E) If OIT identifies an issue of concern in which PII of an individual that posted it is not necessary, the PII will be redacted from any notifications or products that are produced or stored. If PII is deemed relevant, the notifications and work products containing the PII will be retained in AFI.

The DHS Privacy Office finds this is a privacy sensitive use of social media, and requires PIA coverage. Coverage for instances where CBP would identify an issue of concern on social media in which PII is not relevant or necessary is provided by DHS/ALL/PIA-056 DHS and Component Network IT Security Operations and Privacy and IT Security Incident Response, which outlines the Department's efforts to protect the confidentiality, integrity, and availability of DHS information and information assets. In the event that PII is relevant and would be included in notifications and work products, coverage is provided by DHS/CBP/PIA-010(a) Analytical Framework for Intelligence, which discusses information collected as part of CBP's efforts to identify, apprehend, and prosecute individuals who pose a potential law enforcement or security risk, and aids in the enforcement of customs, immigration, and other laws enforced by DHS.

SORN coverage is also required, and is provided by DHS/CBP-024 CIRS, which covers information collected to identify, apprehend, or prosecute individuals who pose a potential law enforcement or security risk.