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.

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

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: 6/12/18

Name of Component: Customs and Border Protection

Contact Information: (b) (6), (b) (7)(C) **International Trade Specialist, Office of Trade,** (b) (6), (b) (7)(C) **International Trade Specialist, Office of Trade** (b) (6), (b) (7)(C) **International Trade Specialist, Office of Trade** (b) (6), (b) (7)(C) (b) (6), (b) (7)(C) **International Trade Specialist, Office of Trade,** (b) (6), (b) (7)(C) **Management and Program Analyst, Office of Trade** (b) (6), (b) (7)(C)

Counsel[2] Contact Information: (b) (6), (b) (7)(C) **Director Forced Labor Division** (b) (6), (b) (7)(C) (b) (6), (b) (7)(C)

IT System(s) where social media data is stored: Information will be stored in users shared drive

Applicable Privacy Impact Assessment(s) (PIA):

- **The CBP Privacy Office finds that overarching PIA coverage for this effort is provided by the DHS/CBP/PIA-010(a) Analytical Framework for Intelligence, which outlines CBPs 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. The CBP Privacy Office is working to develop more specific coverage in the future, however AFI covers 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-017 – Analytical Framework for Intelligence System (June 7, 2012 77 FR 13813), which describes CBP's collection, maintenance, and use of records in order to identify, apprehend, and/or prosecute individuals who pose a potential law enforcement risk and aid in the enforcement of the customs laws.**
- **The CBP Privacy Office finds that SORN coverage for this effort is provided by DHS/CBP-001 Import Information System (July 26, 2016, 81 FR 48826), which describes**

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

CBP's collection, maintenance, and use of records on all commercial goods imported into the United States, along with carrier, broker, importer, as well as other information that facilitates the flow of legitimate shipments, and assists DHS/CBP in securing U.S. borders and targeting illicit goods.

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.**

CBP is submitting this SMOUT to outline the Office of Trade, Forced Labor Division's (FLD) operational use of social media, including (b) (7)(E) capabilities to identify and support FLD cases. The Commissioner of CBP established the Forced Labor Division in 2018 to focus solely on developing forced labor enforcement cases. These cases are (b) (7)(E) (b) (7)(E)

The cases are developed through open source searches (b) (7)(E)

(b) (7)(E) FLD may take notes containing PII from the social media that is reviewed, but it will not be retrievable by a personal identifier. All notes would be stored in password protected files on a shared drive. Because FLD investigates entities, this information will be stored for the length of the investigation.

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

Under the authority of 19 CFR § 12.42 Findings of Commissioner of Customs.

(a) If any port director or other principal Customs officer has reason to believe that any class of merchandise that is being, or is likely to be, imported into the United States is being produced, whether by mining, manufacture, or other means, in any foreign locality with the use of convict labor, forced labor, or indentured labor under penal sanctions, including forced child labor or indentured child labor under penal sanctions, so as to come within the purview of section 307, Tariff Act of 1930, he shall communicate his belief to the Commissioner of Customs. Every such communication shall contain or be accompanied by a statement of substantially the same information as is required in paragraph (b) of this

section, if in the possession of the port director or other officer or readily available to him. Also, under 19 U.S. Code § 1307 - Convict-made goods; importation prohibited. All goods, wares, articles, and merchandise mined, produced, or manufactured wholly or in part in any foreign country by convict labor or/and forced labor or/and indentured labor under penal sanctions shall not be entitled to entry at any of the ports of the United States, and the importation thereof is hereby prohibited, and the Secretary of the Treasury is authorized and directed to prescribe such regulations as may be necessary for the enforcement of this provision.

"Forced labor", as herein used, shall mean all work or service which is exacted from any person under the menace of any penalty for its nonperformance and for which the worker does not offer himself voluntarily. For purposes of this section, the term "forced labor or/and indentured labor" includes forced or indentured child labor.

(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.**

   - **See attached Rules of Behavior (RoB)**

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)

[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;

(b) (7)(E)

[redacted]

d) *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 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: 9/24/18

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/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-001 Import Information System, July 26, 2016, 81 FR 48826; DHS/CBP-017 Analytical Framework for Intelligence System, June 7, 2012, 77 FR 13813
  - ☐ New.
  - ☐ Updated. <Please include the name and number of SORN to be updated here.>

DHS PRIVACY OFFICE COMMENTS

CBP Office of Trade, Forced Labor Division's (FLD) is submitting this SMOUT to discuss the request for access to social media for certain instances to use (b) (7)(E)

(b) (7)(E)

CBP's definition of (b) (7)(E)

(b) (7)(E)

The cases are developed through open source searches to (b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

Under no circumstance will DHS/CBP violate any social media privacy settings. (b) (7) (E)

PIA coverage for this collection is provided by the DHS/CBP/PIA-010(a) Analytical Framework for Intelligence, which outlines CBPs 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. The DHS Privacy Office agrees with CBP Privacy that they should work to develop more specific coverage in the future.

SORN coverage for collection, maintenance, and sharing of information by FLD is provided by DHS/CBP-017 Analytical Framework for Intelligence System (June 7, 2012 77 FR 13813), which describes CBP's collection, maintenance, and use of records in order to identify, apprehend, and/or prosecute individuals who pose a potential law enforcement risk and aid in the enforcement of the customs laws.

Additional SORN coverage is provided by DHS/CBP-001 Import Information System (July 26, 2016, 81 FR 48826), which describes CBP's collection, maintenance, and use of records on all commercial goods imported into the United States, along with carrier, broker, importer, as well as other information that facilitates the flow of legitimate shipments, and assists DHS/CBP in securing U.S. borders and targeting illicit goods.