# TALKING POINTS: OCTOBER 2016 ELECTRONIC SYSTEM FOR TRAVEL AUTHORIZATION ENHANCEMENTS

- In order to further enhance the security of the Visa Waiver Program (VWP), the Department of Homeland Security (DHS) is adding an optional question on social media identifiers (or "handles") on the application of foreign nationals who apply for an Electronic System for Travel Authorization (ESTA).

- The change will affect nonimmigrant visitors seeking to travel to the United States under the VWP who complete the online ESTA application.

- The submission of social media information is voluntary. If an applicant chooses not to fill out or answer questions regarding social media, it will not adversely affect the submission of the ESTA application.

- Information found in social media will be used to review ESTA applications to validate legitimate travel and to identify potential threats.
    - It may help facilitate legitimate travel by providing an additional means to adjudicate issues related to relevant questions about identity, occupation, previous travel, and other factors.
    - Intelligence and investigations show that immediate availability of this information may help to prevent and disrupt current terrorist plots.

- Social media is a prominent component of modern society, and DHS's efforts to protect the homeland must evolve as society evolves. Given the nature of DHS's mission, it would be irresponsible for DHS not to ask for and review this information in DHS's vetting programs.

- DHS's proposal enhances security while protecting privacy. If an applicant chooses to answer this question, DHS will have timely visibility of the publicly available information on those platforms, consistent with the privacy settings the applicant has set on the platforms. Therefore, the hosting provider will not be asked to violate any privacy settings or policies.

- Highly trained U.S. Customs and Border Protection (CBP) officers may review publicly available social media information as an additional data point to assist in CBP's vetting of an ESTA application. CBP will make case-by-case determinations based on the totality of the circumstances.

## IF ASKED

***Q: What is a social media identifier?***

A: A social media identifier is any name, or "handle", used by the individual on platforms including, but not limited to, Facebook, Twitter, and Instagram, among others.

***Q: What if applicants participate in multiple online platforms? Are they being asked to list all of their identifiers, or only one?***

A: Applicants are able to volunteer up to 10 identifiers.

***Q: How will social media information be used for security vetting purposes?***

A: Highly trained U.S. Customs and Border Protection (CBP) officers may review publicly available social media information as an additional data point to assist in CBP's vetting of an ESTA application. CBP will make case-by-case determinations based on the totality of the circumstances.

CBP Officers, Agents, and analysts conducting social media vetting and screening related to the ESTA program are trained on the use of the relevant tools employed in support of the mission and are given additional training on operational security and open source research best practices. They are required to abide by guidelines for the proper use of social media information and research in accordance with CBP's social media rules of behavior, as well as the relevant Social Media Operational Use Template (SMOUT) authorizing them to utilize social media research in their respective roles.

***Q: Will U.S. citizens or Lawful Permanent Residents be asked to provide social media information?***

A: No. ESTA is only for foreign nationals of VWP member countries who wish to travel to the United States under the VWP.

***Q: Why is it not mandatory for individuals to provide their social media identifiers?***

A: The question is voluntary because not all applicants have a social media account and may otherwise choose not to provide this information. If an applicant does not answer the question, or they simply do not hold such an account, the ESTA application can still be successfully submitted.

***Q: Will an ESTA application be denied if the applicant chooses not to provide social media information? What if they don't have a social media account?***

A: No, providing this information is voluntary. If an applicant chooses not to fill out or answer questions regarding social media, the ESTA application can still be successfully submitted.

***Q: Will applicants be contacted by DHS using social media?***

A: DHS already collects and uses email addresses on the ESTA form to communicate with ESTA users; possible future forms of outreach may include contact through social media, if preferred by the applicant.

***Q: Does the collection of social media information violate individual privacy?***

A: No. The ESTA application instructs applicants that social media fields are optional. If an applicant chooses not to fill out or answer the question regarding social media, the ESTA application can still be successfully submitted. If they do choose to answer this question, highly trained CBP personnel will have timely visibility of the publicly available information on those platforms, consistent with the privacy settings the applicant has set on the platforms.

In addition, prior to the inclusion of social media identifiers on the ESTA application, DHS will post an updated Privacy Impact Assessment (PIA) and System of Record Notice (SORN) for ESTA on the DHS website (www.dhs.gov/privacy) to provide notice and assess the privacy risks associated with enhancements to the ESTA application questionnaire, including the addition of an optional field for social media usernames or identifiers for all ESTA applicants. Information collected under the ESTA program will be maintained and handled in accordance with the Privacy Act and relevant SORNs.

***Q: Will collecting social media data target a particular population based on political views, race, ethnicity, or religion?***

A: No. DHS is steadfastly committed to the highest standards of conduct across the Department, most acutely when it comes to the fair, unbiased, and transparent enforcement of our laws. Consistent with DHS's mission to secure the Nation from threats and facilitate legitimate trade and travel, the collection of social media identifiers will not be used to prevent travel based on applicant's political views, race, ethnicity, or religion. These factors are not relevant in determining admissibility and/or eligibility to travel under the Visa Waiver Program.

***Q: Does screening using social media data violate freedom of speech?***

A: No. The collection of social media identifiers will not be used to prevent travel based on an applicant's political views, race, ethnicity, or religion.

***Q: How will the collected social media information be safeguarded and stored?***

A: The collected social media information will be safeguarded and stored in accordance with the ESTA SORN, which will be published in the Federal Register prior to collecting social media information.

***Q: How long will the USG retain social media information?***

A: The collected social media information will be safeguarded and stored in accordance with the ESTA SORN, which will be published in the Federal Register and posted on the DHS website (www.dhs.gov/privacy) prior to collecting social media information.

Privacy Office
U S Department of Homeland Security
Washington, DC 20528
202 (b) (7)(E) @dhs gov
www dhs gov/privacy



# PRIVACY THRESHOLD ANALYSIS (PTA)

**This form is used to determine whether a Privacy Impact Assessment is required.**

Please use the attached form to determine whether a Privacy Impact Assessment (PIA) is required under the E-Government Act of 2002 and the Homeland Security Act of 2002.

Please complete this form and send it to your component Privacy Office. If you do not have a component Privacy Office, please send the PTA to the DHS Privacy Office:

Senior Director, Privacy Compliance
The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
Tel: 202 (b) (7)(E)

(b) (7)(E)@hq.dhs.gov

Upon receipt from your component Privacy Office, the DHS Privacy Office will review this form. If a PIA is required, the DHS Privacy Office will send you a copy of the Official Privacy Impact Assessment Guide and accompanying Template to complete and return.

A copy of the Guide and Template is available on the DHS Privacy Office website, www.dhs.gov/privacy, on DHSConnect and directly from the DHS Privacy Office via email: (b) (7)(E)@hq.dhs.gov, phone: 202 (b) (7)(E)

Privacy Office
U S Department of Homeland Security
Washington, DC 20528
202- (b) (7)(E) @dhs gov
www dhs gov/privacy



# PRIVACY THRESHOLD ANALYSIS (PTA)

## SUMMARY INFORMATION

| | | | |
|---|---|---|---|
| **Project or Program Name:** | **IntelCenter Social Media Database Ingestion into ATS** | | |
| **Component:** | Customs and Border Protection (CBP) | **Office or Program:** | OFO (b) (7)(E) |
| **Xacta FISMA Name (if applicable):** | **Automated Targeting System (ATS)** | **Xacta FISMA Number (if applicable):** | (b) (7)(E) |
| **Type of Project or Program:** | **IT System** | **Project or program status:** | **Pilot** |
| **Date first developed:** | **January 10, 2017** | **Pilot launch date:** | |
| **Date of last PTA update** | **N/A** | **Pilot end date:** | **July 1, 2018** |
| **ATO Status (if applicable)** | Choose an item. | **ATO expiration date (if applicable):** | Click here to enter a date. |

## PROJECT OR PROGRAM MANAGER

| | | | |
|---|---|---|---|
| **Name:** | (b) (6), (b) (7)(C) | | |
| **Office:** | **OFO** | **Title:** | Director |
| **Phone:** | (b) (6), (b) (7)(C) | **Email:** | (b) (6), (b) (7)(C) @cbp.dhs.gov |

## INFORMATION SYSTEM SECURITY OFFICER (ISSO) (IF APPLICABLE)

| | | | |
|---|---|---|---|
| **Name:** | (b) (6), (b) (7)(C) | | |
| **Phone:** | (b) (6), (b) (7)(C) | **Email:** | (b) (6), (b) (7)(C) @associates.dhs.gov |

## SPECIFIC PTA QUESTIONS

1. Reason for submitting the PTA: New PTA

CBP has entered into contract with IntelCenter, a private database vendor, to test and evaluate whether IntelCenter's database of social media and open source selectors (b) (7)(E), (b) (4) [redacted] may assist CBP targeting, vetting, and screening efforts. (b) (7)(E) [redacted]

Under this proof-of-concept study, the information will primarily be used by the (b) (7)(E) for (b) (7)(E) [redacted]. (b) (7)(E)

(b) (4), (b) (7)(E) [redacted]

(b) (4), (b) (7)(E) [redacted]

Analysis during this testing and evaluation pilot will be focused primarily on (b) (7)(E) However, research using publicly available information may be conducted on (b) (7)(E) pursuant to CBP's law enforcement authorities as deemed necessary to support CBP operations. As a pilot, this study will be fluid and allow for a range of information to be researched.

The IntelCenter database will give CBP personnel focused on open source and publicly available information research additional insight into (b) (7)(E)

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

At or before the end of the pilot on July 1, 2018, information from IntelCenter (b) (7)(E) [redacted]
(b) (7)(E) (b) (5), (b) (7)(E) [redacted]

(b) (7)(E), (b) (4), (b) (5) [redacted]

Information from IntelCenter (b) (7)(E) [redacted] will be maintained consistent with the ATS retention schedule. **No information will be shared with IntelCenter during or after this pilot.**

| | |
|---|---|
| **2. Does this system employ any of the following technologies:**<br>*If you are using any of these technologies and want coverage under the respective PIA for that technology please stop here and contact the DHS Privacy Office for further guidance.* | ☐ Closed Circuit Television (CCTV)<br>☒ Social Media<br>☐ Web portal[1] (e.g., SharePoint)<br>☐ Contact Lists<br>☐ None of these |

| | |
|---|---|
| **3. From whom does the Project or Program collect, maintain, use, or disseminate information?**<br>*Please check all that apply.* | ☐ This program does not collect any personally identifiable information[2]<br>☒ Members of the public<br>☐ DHS employees/contractors (list components):<br>☐ Contractors working on behalf of DHS<br>☐ Employees of other federal agencies |

**4. What specific information about individuals is collected, generated or retained?**

(b) (4), (b) (7)(E) [redacted]

[1] Informational and collaboration-based portals in operation at DHS and its components that collect, use, maintain, and share limited personally identifiable information (PII) about individuals who are "members" of the portal or "potential members" who seek to gain access to the portal.

[2] DHS defines personal information as "Personally Identifiable Information" or PII, which is any information that permits the identity of an individual to be directly or indirectly inferred, including any information that is linked or linkable to that individual, regardless of whether the individual is a U.S. citizen, lawful permanent resident, visitor to the U.S., or employee or contractor to the Department. "Sensitive PII" is PII, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. For the purposes of this PTA, SPII and PII are treated the same.

(b) (7)(E), (b) (4)

**CBP will only ingest** (b) (7)(E), (b) (4) **as part of this effort.**

In the event of a match, (b) (7)(E), (b) (4) will be uploaded into ATS. This data will be used to (b) (7)(E)

(b) (7)(E)

(b) (4), (b) (7)(E)

| | |
|---|---|
| **4(a) Does the project, program, or system retrieve information by personal identifier?** | ☐ No. Please continue to next question.<br>☒ Yes. If yes, please list all personal identifiers used:<br>See list in section 4 |
| **4(b) Does the project, program, or system use Social Security Numbers (SSN)?** | ☒ No.<br>☐ Yes. |
| **4(c) If yes, please provide the specific legal basis and purpose for the collection of SSNs:** | N/A |
| **4(d) If yes, please describe the uses of the SSNs within the project, program, or system:** | N/A |
| **4(e) If this project, program, or system is an information technology/system, does it relate solely to infrastructure?** | ☒ No. Please continue to next question. |

| | |
|---|---|
| *For example, is the system a Local Area Network (LAN) or Wide Area Network (WAN)?* | ☐ Yes. If a log kept of communication traffic, please answer the following question. |
| **4(f) If header or payload data[3] is stored in the communication traffic log, please detail the data elements stored.** | |
| Click here to enter text.<br>N/A | |

| | |
|---|---|
| **5. Does this project, program, or system connect, receive, or share PII with any other DHS programs or systems[4]?** | ☐ No.<br>☒ Yes. If yes, please list:<br>(b) (4), (b) (7)(E) |
| **6. Does this project, program, or system connect, receive, or share PII with any external (non-DHS) partners or systems?** | ☐ No.<br>☒ Yes. If yes, please list:<br>(b) (4), (b) (7)(E) |
| **6(a) Is this external sharing pursuant to new or existing information sharing access agreement (MOU, MOA, LOI, etc.)?** | N/A |
| **7. Does the project, program, or system provide role-based training for personnel who have access in addition to annual privacy training required of all DHS personnel?** | ☐ No.<br>☒ Yes. If yes, please list: CBP personnel using this database are required to act in accordance with CBP's existing authorities and in compliance with the CBP Social Media Directive (including completing the required training) and Social Media Rules of Behavior. |

[3] When data is sent over the Internet, each unit transmitted includes both header information and the actual data being sent. The header identifies the source and destination of the packet, while the actual data is referred to as the payload. Because header information, or overhead data, is only used in the transmission process, it is stripped from the packet when it reaches its destination. Therefore, the payload is the only data received by the destination system.

[4] PII may be shared, received, or connected to other DHS systems directly, automatically, or by manual processes. Often, these systems are listed as "interconnected systems" in Xacta.

| | |
|---|---|
| **8. Per NIST SP 800-53 Rev. 4, Appendix J, does the project, program, or system maintain an accounting of disclosures of PII to individuals/agencies who have requested access to their PII?** | ☐<br><br>☒ Yes. In what format is the accounting maintained: If information from IntelCenter is disseminated outside of DHS, it will be pursuant to an MOU, or a DHS 191 Form will be provided to the CBP Privacy and Diversity Office. In addition, ATS maintains an audit trail. |
| **9. Is there a FIPS 199 determination?[4]** | ☐ Unknown.<br>☐ No.<br>☒ Yes. Please indicate the determinations for each of the following:<br><br>Confidentiality:<br>☐ Low ☒ Moderate ☐ High ☐ Undefined<br><br>Integrity:<br>☐ Low ☒ Moderate ☐ High ☐ Undefined<br><br>Availability:<br>☐ Low ☒ Moderate ☐ High ☐ Undefined |

## PRIVACY THRESHOLD REVIEW

## (TO BE COMPLETED BY COMPONENT PRIVACY OFFICE)

| | |
|---|---|
| **Component Privacy Office Reviewer:** | (b) (6), (b) (7)(C) |
| **Date submitted to Component Privacy Office:** | **May 21, 2017** |
| **Date submitted to DHS Privacy Office:** | June 30, 2017 |
| **Component Privacy Office Recommendation:**<br>*Please include recommendation below, including what new privacy compliance documentation is needed.* | |

[4] FIPS 199 is the Federal Information Processing Standard Publication 199, Standards for Security Categorization of Federal Information and Information Systems and is used to establish security categories of information systems.

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

[redacted]

**(TO BE COMPLETED BY THE DHS PRIVACY OFFICE)**

| | |
|---|---|
| **DHS Privacy Office Reviewer:** | (b) (6), (b) (7)(C) |
| **PCTS Workflow Number:** | (b) (7)(E) |
| **Date approved by DHS Privacy Office:** | July 12, 2017 |
| **PTA Expiration Date** | July 12, 2018 |

**DESIGNATION**

| | |
|---|---|
| **Privacy Sensitive System:** | Yes If "no" PTA adjudication is complete. |
| **Category of System:** | IT System<br>If "other" is selected, please describe: Click here to enter text. |
| **Determination:** | ☐ PTA sufficient at this time.<br>☐ Privacy compliance documentation determination in progress.<br>☐ New information sharing arrangement is required.<br>☐ DHS Policy for Computer-Readable Extracts Containing Sensitive PII applies. |

| | |
|---|---|
| | ☐ Privacy Act Statement required.<br>☒ Privacy Impact Assessment (PIA) required.<br>☒ System of Records Notice (SORN) required.<br>☐ Paperwork Reduction Act (PRA) Clearance may be required. Contact your component PRA Officer.<br>☐ A Records Schedule may be required. Contact your component Records Officer. |
| **PIA:** | **PIA update is required.**<br>If covered by existing PIA, please list: DHS/CBP/PIA-006 Automated Targeting System (ATS) |
| **SORN:** | System covered by existing SORN<br>If covered by existing SORN, please list: DHS/CBP-006 Automated Targeting System, May 22, 2012, 77 FR 30297 |

**DHS Privacy Office Comments:**
*Please describe rationale for privacy compliance determination above.*

CBP is submitting this PTA to discuss a new sharing arrangement with IntelCenter, a private database vendor, to test and evaluate whether the vendor's database of social media (b) (4), (b) (7)(E) may assist CBP targeting, vetting, and screening efforts. (b) (7)(E)

The information will be used by the (b) (7)(E) for CBP will (b) (7)(E)

(b) (4), (b) (7)(E)

(b) (7)(E)

(b) (7)(E)

The DHS Privacy Office agrees that the ingestion of data from IntelCenter is privacy-sensitive due to the collection of information from members of the public. A PIA Update to DHS/CBP/PIA-006 Automated Targeting System (ATS) is required to describe the initiative. SORN coverage is provided by DHS/CBP-006 Automated Targeting System.

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

In all cases involved in this pilot, CBP will access publicly available information in accordance with the privacy policies of the underlying social media or open source platforms analyzed. This means that all searches (b) (7)(E) will be consistent with the purposes already approved in CBP's SMOUTs.

Privacy Office
U S Department of Homeland Security
Washington, DC 20528
202 (b) (7)(E) @dhs gov
www dhs gov/privacy



# PRIVACY THRESHOLD ANALYSIS (PTA)

**This form is used to determine whether a Privacy Impact Assessment is required.**

Please use the attached form to determine whether a Privacy Impact Assessment (PIA) is required under the E-Government Act of 2002 and the Homeland Security Act of 2002.

Please complete this form and send it to your component Privacy Office. If you do not have a component Privacy Office, please send the PTA to the DHS Privacy Office:

Senior Director, Privacy Compliance
The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
Tel: 202 (b) (7)(E)

(b) (7)(E) @hq.dhs.gov

Upon receipt from your component Privacy Office, the DHS Privacy Office will review this form. If a PIA is required, the DHS Privacy Office will send you a copy of the Official Privacy Impact Assessment Guide and accompanying Template to complete and return.

A copy of the Guide and Template is available on the DHS Privacy Office website, www.dhs.gov/privacy, on DHS Connect and directly from the DHS Privacy Office via email: (b) (7)(E) @hq.dhs.gov, phone: 202 (b) (7)(E)

## PRIVACY THRESHOLD ANALYSIS (PTA)

### SUMMARY INFORMATION

| | | | |
|---|---|---|---|
| **Project or Program Name:** | (b) (7)(E) | | |
| **Component:** | Customs and Border Protection (CBP) | **Office or Program:** | **Office of Intelligence and the Office of Professional Responsibility** |
| **Xacta FISMA Name (if applicable):** | | **Xacta FISMA Number (if applicable):** | Click here to enter text. |
| **Type of Project or Program:** | **Pilot** | **Project or program status:** | **Pilot** |
| **Date first developed:** | **March 12, 2018** | **Pilot launch date:** | **March 12, 2018** |
| **Date of last PTA update** | **March 12, 2018** | **Pilot end date:** | Click here to enter a date. |
| **ATO Status (if applicable)** | **Not started** | **ATO expiration date (if applicable):** | Click here to enter a date. |

### PROJECT OR PROGRAM MANAGER

| | | | |
|---|---|---|---|
| **Name:** | (b) (6), (b) (7)(C) | | |
| **Office:** | **Office of Intelligence** | **Title:** | PM |
| **Phone:** | (b) (6), (b) (7)(C) | **Email:** | (b) (6), (b) (7)(C) |

### INFORMATION SYSTEM SECURITY OFFICER (ISSO) (IF APPLICABLE)

| | | | |
|---|---|---|---|
| **Name:** | Click here to enter text. | | |
| **Phone:** | Click here to enter text. | **Email:** | Click here to enter text. |

## SPECIFIC PTA QUESTIONS

**1. Reason for submitting the PTA: New PTA**

This PTA outlines the support U.S. Customs and Border Protection's (b) (7)(E) will provide to the (b) (7)(E) a joint endeavor between the Office of Intelligence (OI) and the Office of Professional Responsibility (OPR), to monitor social media in an effort to identify (b) (7)(E)

Background: (b) (7)(E) involves a (b) (7)(E)

*Concept*: The monitoring of Social Media (b) (7)(E) will identify (b) (7)(E) will help CBP assess security needs, as well as help the (b) determine if social media monitoring is a useful tool for (b) (7)(E)

*Duration*: Starting (b) (7)(E) through the (b) (7)(E), or sooner, as determined by the (b) (7)(E)

*Informational Use*:

a. Initial information will aid CBP's Assistant Commissioners of OPR and OI in providing information to the Commissioner of CBP, and subsequently the United States Marshal Service, (b) (7)(E)

b. Information gathered during the (b) may identify (b) (7)(E)

c. Any discovered threat information will be reported through the Joint Intake Center.

d. Personally Identifiable Information (PII), including but not limited to screennames, social media handles, and IP address will not be collected unless (b) (7)(E) in collaboration with the Joint Intake Center.

e. No monitoring of, or reporting on, First Amendment protected speech or activities will occur. However, if such activities (b) (7)(E) reporting will be conducted through the Joint Intake Center.

*Gathering of the Information:*

CBP's (b) (7)(E) will provide personnel specifically trained to access, use, and protect PII when accessing social media monitoring. (b) (7) personnel will report (b) to the Office of Professional Responsibility, and the Office of Intelligence, who will upload it into the Joint Intake Center. (7

| | |
|---|---|
| **2. Does this system employ any of the following technologies:**<br>*If you are using any of these technologies and want coverage under the respective PIA for that technology please stop here and contact the DHS Privacy Office for further guidance.* | ☐ Closed Circuit Television (CCTV)<br>☒ Social Media<br>☐ Web portal[1] (e.g., SharePoint)<br>☐ Contact Lists<br>☐ None of these |

| | |
|---|---|
| **3. From whom does the Project or Program collect, maintain, use, or disseminate information?**<br>*Please check all that apply.* | ☐ This program does not collect any personally identifiable information[2]<br>☒ Members of the public<br>☐ DHS employees/contractors (list components):<br>☐ Contractors working on behalf of DHS<br>☐ Employees of other federal agencies |

**4. What specific information about individuals is collected, generated or retained?**

Information gathered from Social Media (SM) (to include but not limited to):

a. (b) (7)(E)

b.

c.

[1] Informational and collaboration-based portals in operation at DHS and its components that collect, use, maintain, and share limited personally identifiable information (PII) about individuals who are "members" of the portal or "potential members" who seek to gain access to the portal.

[2] DHS defines personal information as "Personally Identifiable Information" or PII, which is any information that permits the identity of an individual to be directly or indirectly inferred, including any information that is linked or linkable to that individual, regardless of whether the individual is a U.S. citizen, lawful permanent resident, visitor to the U.S., or employee or contractor to the Department. "Sensitive PII" is PII, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. For the purposes of this PTA, SPII and PII are treated the same.

| | |
|---|---|
| d. (b) (7)(E) | |
| **4(a) Does the project, program, or system retrieve information by personal identifier?** | ☐ No. Please continue to next question.<br>☒ Yes. If yes, please list all personal identifiers used: (b) (7)(E) (b) (7)(E) |
| **4(b) Does the project, program, or system use Social Security Numbers (SSN)?** | ☒ No.<br>☐ Yes. |
| **4(c) If yes, please provide the specific legal basis and purpose for the collection of SSNs:** | |
| **4(d) If yes, please describe the uses of the SSNs within the project, program, or system:** | |
| **4(e) If this project, program, or system is an information technology/system, does it relate solely to infrastructure?**<br>*For example, is the system a Local Area Network (LAN) or Wide Area Network (WAN)?* | ☐ No. Please continue to next question.<br>☒ Yes. If a log kept of communication traffic, please answer the following question. |
| **4(f) If header or payload data[3] is stored in the communication traffic log, please detail the data elements stored.** | |
| Click here to enter text. | |

| | |
|---|---|
| **5. Does this project, program, or system connect, receive, or share PII with any other DHS programs or systems[4]?** | ☐ No.<br>☒ Yes. If yes, please list: (b) (7)(E) will be reported through the Joint Intake Center |

[3] When data is sent over the Internet, each unit transmitted includes both header information and the actual data being sent. The header identifies the source and destination of the packet, while the actual data is referred to as the payload. Because header information, or overhead data, is only used in the transmission process, it is stripped from the packet when it reaches its destination. Therefore, the payload is the only data received by the destination system.

[4] PII may be shared, received, or connected to other DHS systems directly, automatically, or by manual processes. Often, these systems are listed as "interconnected systems" in Xacta.

| | |
|---|---|
| **6. Does this project, program, or system connect, receive, or share PII with any external (non-DHS) partners or systems?** | ☐ No.<br>☒ Yes. If yes, please list: United States Marshal Service (USMS) |
| **6(a) Is this external sharing pursuant to new or existing information sharing access agreement (MOU, MOA, LOI, etc.)?** | Choose an item.<br>Please describe applicable information sharing governance in place: |
| **7. Does the project, program, or system provide role-based training for personnel who have access in addition to annual privacy training required of all DHS personnel?** | ☐ No.<br>☒ Yes. If yes, please list: (b) (7)(E) provides personnel with access to social media information with specific training related to access, use, and protection of PII. |
| **8. Per NIST SP 800-53 Rev. 4, Appendix J, does the project, program, or system maintain an accounting of disclosures of PII to individuals who have requested access to their PII?** | ☐ No. What steps will be taken to develop and maintain the accounting:<br>☐ Yes. In what format is the accounting maintained: |
| **9. Is there a FIPS 199 determination?[4]** | ☒ Unknown.<br>☐ No.<br>☐ Yes. Please indicate the determinations for each of the following:<br>Confidentiality:<br>☐ Low ☐ Moderate ☐ High ☐ Undefined<br>Integrity:<br>☐ Low ☐ Moderate ☐ High ☐ Undefined<br>Availability:<br>☐ Low ☐ Moderate ☐ High ☐ Undefined |

[4] FIPS 199 is the Federal Information Processing Standard Publication 199, Standards for Security Categorization of Federal Information and Information Systems and is used to establish security categories of information systems.

Privacy Office
U S Department of Homeland Security
Washington, DC 20528
202 (b) (7)(E) @dhs gov
www dhs gov/privacy



## PRIVACY THRESHOLD REVIEW

## (TO BE COMPLETED BY COMPONENT PRIVACY OFFICE)

| | |
|---|---|
| **Component Privacy Office Reviewer:** | (b) (6), (b) (7)(C) |
| **Date submitted to Component Privacy Office:** | **March 13, 2018** |
| **Date submitted to DHS Privacy Office:** | March 13, 2018 |

**Component Privacy Office Recommendation:**
*Please include recommendation below, including what new privacy compliance documentation is needed.*

(b) (5)

(b) (7)(E)

(7)

(b) (5)

**(TO BE COMPLETED BY THE DHS PRIVACY OFFICE)**

| | |
|---|---|
| **DHS Privacy Office Reviewer:** | (b) (6), (b) (7)(C) |
| **PCTS Workflow Number:** | (b) (7)(E) |
| **Date approved by DHS Privacy Office:** | March 14, 2018 |
| **PTA Expiration Date** | End of (b) |

**DESIGNATION**

| | |
|---|---|
| **Privacy Sensitive System:** | Yes If "no" PTA adjudication is complete. |
| **Category of System:** | IT System<br>If "other" is selected, please describe: Click here to enter text. |
| **Determination:** | ☐ PTA sufficient at this time.<br>☐ Privacy compliance documentation determination in progress.<br>☐ New information sharing arrangement is required.<br>☐ DHS Policy for Computer-Readable Extracts Containing Sensitive PII applies.<br>☐ Privacy Act Statement required.<br>☒ Privacy Impact Assessment (PIA) required.<br>☒ System of Records Notice (SORN) required.<br>☐ Paperwork Reduction Act (PRA) Clearance may be required. Contact your component PRA Officer.<br>☐ A Records Schedule may be required. Contact your component Records Officer. |
| **PIA:** | **System covered by existing PIA**<br>If covered by existing PIA, please list: DHS/CBP/PIA-044 Joint Integrity Case Management System (JICMS) |
| **SORN:** | System covered by existing SORN |

| | |
|---|---|
| | If covered by existing SORN, please list: DHS/CBP-024 Intelligence Records System (CIRS) System of Records, September 21, 2017, 82 FR 44198 |

**DHS Privacy Office Comments:**
*Please describe rationale for privacy compliance determination above.*

CBP is submitting this PTA to discuss the (b) (7)(E) use of social media in support of the Office of Professional Responsibility (OPR) (b) (7)(E) (b) (7)(E) and the Office of Intelligence. The goal of this initiative is to (b) (7)(E) (who is the (b) (7)(E) ) (b) during the upcoming (b) This effort will be used as a test case for determining the value of social media as part of the overarching effort of (b) to (b) (7)(E) .

The (b) (7)(E) will be conducting the search of publicly available social media information that constitutes (b) (7)(E) . The (b) will use PII from the (b) (7)(E) to (b) (7)(E) . During the search process, PII that may be collected includes names, screen names/handles, email addresses, and other common identifiers associated with an individual's online presence (b) (7)(E) associated with the (b) Once identified, (b) will pass the information to the Office of Professional Responsibility, and the Office of Intelligence, who will upload it into the Joint Intake Center.

The DHS Privacy Office agrees that this initiative is privacy-sensitive, requiring PIA and SORN coverage.

PIA coverage is provided by DHS/CBP/PIA-044 Joint Integrity Case Management System (JICMS), which is CBP's system for managing criminal and administrative investigations, including (b) (7)(E) SORN coverage is provided by DHS/CBP-024 Intelligence Records System (CIRS), which outlines the collection and consolidation of information from various sources (including social media) in order to enhance CBP's ability to identify, apprehend, or prosecute individuals who pose a potential law enforcement or security risk.

**CBP is required to submit a new PTA if** (b) (5), (b) (7)(E) **:**

While (b) (7)(E) provides personnel with access to social media information with specific training related to access, use, and protection of PII, (b) (5) (b) (5), (b) (7)(E) (b) (5)

**During this use case, CBP should understand the prohibitions surrounding collection of 1st Amendment-protected speech and activities**, such as protest, pursuant to 5 U.S.C. § 552a(e)(7) requiring that agencies "maintain no record describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual about whom the record is maintained or unless pertinent to and within the scope of an authorized law enforcement activity." During this use case, CBP will exercise the judicial "law enforcement activity" exception due to a) the limited nature in which (b) (7)(E) is collecting information in order to (b) (7)(E) directed at the (b) (7)(E) and CBP assets (b) (7)(E); and b) the limited timeframe of the potential collection (limited to the (b) (7)(E) only).

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

Privacy Office
U S Department of Homeland Security
Washington, DC 20528
(b) (6), (b) (7)(C), (b) (7)(E)@dhs gov
www dhs gov/privacy



# PRIVACY THRESHOLD ANALYSIS (PTA)

**This form is used to determine whether a Privacy Impact Assessment is required.**

Please use the attached form to determine whether a Privacy Impact Assessment (PIA) is required under the E-Government Act of 2002 and the Homeland Security Act of 2002.

Please complete this form and send it to your component Privacy Office. If you do not have a component Privacy Office, please send the PTA to the DHS Privacy Office:

Senior Director, Privacy Compliance
The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
Tel: (b) (6), (b) (7)(C)

(b) (7)(E)@hq.dhs.gov

Upon receipt from your component Privacy Office, the DHS Privacy Office will review this form. If a PIA is required, the DHS Privacy Office will send you a copy of the Official Privacy Impact Assessment Guide and accompanying Template to complete and return.

A copy of the Guide and Template is available on the DHS Privacy Office website, www.dhs.gov/privacy, on DHSConnect and directly from the DHS Privacy Office via email: (b) (7)(E)@hq.dhs.gov, phone: (b) (6), (b) (7)(C)

# PRIVACY THRESHOLD ANALYSIS (PTA)

## SUMMARY INFORMATION

| | | | |
|---|---|---|---|
| **Project or Program Name:** | **YouTube Access for CBP** | | |
| **Component:** | Customs and Border Protection (CBP) | **Office or Program:** | OIT |
| **Xacta FISMA Name (if applicable):** | **N/A** | **Xacta FISMA Number (if applicable):** | **N/A** |
| **Type of Project or Program:** | **Pilot** | **Project or program status:** | **Pilot** |
| **Date first developed:** | **December 1, 2017** | **Pilot launch date:** | **December 18, 2017** |
| **Date of last PTA update** | | **Pilot end date:** | **January 31, 2018** |
| **ATO Status (if applicable)** | Choose an item. | **ATO expiration date (if applicable):** | Click here to enter a date. |

## PROJECT OR PROGRAM MANAGER

| | | | |
|---|---|---|---|
| **Name:** | (b) (6), (b) (7)(C) | | |
| **Office:** | **OIT/ENTSD** | **Title:** | Project Manager |
| **Phone:** | (b) (6), (b) (7)(C) | **Email:** | (b) (6), (b) (7)(C) |

## INFORMATION SYSTEM SECURITY OFFICER (ISSO) (IF APPLICABLE)

| | | | |
|---|---|---|---|
| **Name:** | **N/A** | | |
| **Phone:** | | **Email:** | |

## SPECIFIC PTA QUESTIONS

| **1. Reason for submitting the PTA: New PTA** |
|---|
| CBP is submitting this new PTA to document the initial phase in providing CBP personnel access to social media to view training. This initial phase involves providing access to OIT employees at certain CBP facilities to assess the security and network impact of streaming YouTube to the workforce. CBP is not using YouTube to interact with other users nor will it post anything on YouTube, and this does not constitute an operational use case.<br><br>This initial phase is limited to OIT personnel who need to conduct security and infrastructure testing to assess the impacts of expanding YouTube access to the entire CBP workforce. CBP personnel with access to YouTube will not comment or interact with other users on the platform, nor will they use the platform to conduct research related to any individuals. CBP employees accessing YouTube will not store any information on CBP systems. All information viewed as part of this pilot is voluntarily posted by the public on YouTube and is publically available.<br><br>Future phases of the project will involve providing all CBP personnel with access to YouTube and may expand to additional social media sites that provide training. In the future, some employees may also access YouTube for information related to situational awareness. CBP will submit a new Rules of Behavior and an updated PTA or Social Media Operational Use Template as appropriate for these phases. |

| **2. Does this system employ any of the following technologies:**<br>*If you are using any of these technologies and want coverage under the respective PIA for that technology please stop here and contact the DHS Privacy Office for further guidance.* | ☐ Closed Circuit Television (CCTV)<br>☒ Social Media<br>☐ Web portal[1] (e.g., SharePoint)<br>☐ Contact Lists<br>☐ None of these |
|---|---|

| **3. From whom does the Project or Program collect, maintain, use, or disseminate information?**<br>*Please check all that apply.* | ☒ This program does not collect any personally identifiable information[2]<br>☐ Members of the public<br>☐ DHS employees/contractors (list components): |
|---|---|

[1] Informational and collaboration-based portals in operation at DHS and its components that collect, use, maintain, and share limited personally identifiable information (PII) about individuals who are "members" of the portal or "potential members" who seek to gain access to the portal.

[2] DHS defines personal information as "Personally Identifiable Information" or PII, which is any information that permits the identity of an individual to be directly or indirectly inferred, including any information that is linked or linkable to that individual, regardless of whether the individual is a U.S. citizen, lawful permanent resident, visitor to the U.S., or employee or contractor to the Department. "Sensitive PII" is PII, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. For the purposes of this PTA, SPII and PII are treated the same.

| | |
|---|---|
| | ☐ Contractors working on behalf of DHS<br>☐ Employees of other federal agencies |

| **4. What specific information about individuals is collected, generated or retained?** | |
|---|---|
| No information is collected as part of this phase of the pilot, nor will any information be collected by employees who use social media for training purposes. Although personally identifiable information may incidentally be visible to CBP personnel during this pilot, the purpose of the initiative is solely to conduct security and infrastructure testing. | |
| **4(a) Does the project, program, or system retrieve information by personal identifier?** | ☒ No. Please continue to next question.<br>☐ Yes. If yes, please list all personal identifiers used: |
| **4(b) Does the project, program, or system use Social Security Numbers (SSN)?** | ☒ No.<br>☐ Yes. |
| **4(c) If yes, please provide the specific legal basis and purpose for the collection of SSNs:** | Click here to enter text. |
| **4(d) If yes, please describe the uses of the SSNs within the project, program, or system:** | Click here to enter text. |
| **4(e) If this project, program, or system is an information technology/system, does it relate solely to infrastructure?**<br>*For example, is the system a Local Area Network (LAN) or Wide Area Network (WAN)?* | ☒ No. Please continue to next question.<br>☐ Yes. If a log kept of communication traffic, please answer the following question. |
| **4(f) If header or payload data[3] is stored in the communication traffic log, please detail the data elements stored.** | |
| Click here to enter text. | |

[3] When data is sent over the Internet, each unit transmitted includes both header information and the actual data being sent. The header identifies the source and destination of the packet, while the actual data is referred to as the payload. Because header information, or overhead data, is only used in the transmission process, it is stripped from the packet when it reaches its destination. Therefore, the payload is the only data received by the destination system.

| | |
|---|---|
| **5. Does this project, program, or system connect, receive, or share PII with any other DHS programs or systems[4]?** | ☒ No.<br>☐ Yes. If yes, please list:<br>Click here to enter text. |
| **6. Does this project, program, or system connect, receive, or share PII with any external (non-DHS) partners or systems?** | ☒ No.<br>☐ Yes. If yes, please list:<br>Click here to enter text. |
| **6(a) Is this external sharing pursuant to new or existing information sharing access agreement (MOU, MOA, LOI, etc.)?** | Choose an item.<br>Please describe applicable information sharing governance in place: |
| **7. Does the project, program, or system provide role-based training for personnel who have access in addition to annual privacy training required of all DHS personnel?** | ☒ No.<br>☐ Yes. If yes, please list: |
| **8. Per NIST SP 800-53 Rev. 4, Appendix J, does the project, program, or system maintain an accounting of disclosures of PII to individuals who have requested access to their PII?** | ☒ No. What steps will be taken to develop and maintain the accounting:<br>☐ Yes. In what format is the accounting maintained: |
| **9. Is there a FIPS 199 determination?[4]** | ☒ Unknown.<br>☐ No.<br>☐ Yes. Please indicate the determinations for each of the following:<br>Confidentiality:<br>☐ Low ☐ Moderate ☐ High ☐ Undefined<br>Integrity:<br>☐ Low ☐ Moderate ☐ High ☐ Undefined |

[4] PII may be shared, received, or connected to other DHS systems directly, automatically, or by manual processes. Often, these systems are listed as "interconnected systems" in Xacta.
[4] FIPS 199 is the Federal Information Processing Standard Publication 199, Standards for Security Categorization of Federal Information and Information Systems and is used to establish security categories of information systems.

| | |
|---|---|
| | Availability:<br>☐ Low ☐ Moderate ☐ High ☐ Undefined |

## PRIVACY THRESHOLD REVIEW

## (TO BE COMPLETED BY COMPONENT PRIVACY OFFICE)

| | |
|---|---|
| **Component Privacy Office Reviewer:** | (b) (6), (b) (7)(C) |
| **Date submitted to Component Privacy Office:** | **December 18, 2017** |
| **Date submitted to DHS Privacy Office:** | December 18, 2017 |

**Component Privacy Office Recommendation:**
*Please include recommendation below, including what new privacy compliance documentation is needed.*

(b) (5)

[redacted]

[redacted]

[redacted]

## (TO BE COMPLETED BY THE DHS PRIVACY OFFICE)

| | |
|---|---|
| **DHS Privacy Office Reviewer:** | (b) (6), (b) (7)(C) |
| **PCTS Workflow Number:** | (b) (7)(E) |
| **Date approved by DHS Privacy Office:** | December 21, 2017 |
| **PTA Expiration Date** | December 21, 2020 |

## DESIGNATION

| | |
|---|---|
| **Privacy Sensitive System:** | No If "no" PTA adjudication is complete. |

| | |
|---|---|
| **Category of System:** | IT System<br>If "other" is selected, please describe: Click here to enter text. |

**Determination:**

☒ PTA sufficient at this time.

☐ Privacy compliance documentation determination in progress.

☐ New information sharing arrangement is required.

☐ DHS Policy for Computer-Readable Extracts Containing Sensitive PII applies.

☐ Privacy Act Statement required.

☐ Privacy Impact Assessment (PIA) required.

☐ System of Records Notice (SORN) required.

☐ Paperwork Reduction Act (PRA) Clearance may be required. Contact your component PRA Officer.

☐ A Records Schedule may be required. Contact your component Records Officer.

| | |
|---|---|
| **PIA:** | Choose an item.<br>If covered by existing PIA, please list: |
| **SORN:** | Choose an item.<br>If covered by existing SORN, please list: Click here to enter text. |

**DHS Privacy Office Comments:**
*Please describe rationale for privacy compliance determination above.*

CBP Privacy is submitting this PTA to document the initial phase of a pilot assessing the feasibility of allowing CBP employees to access YouTube. This initial phase will open YouTube to certain OIT facilities and users to conduct testing on network and security impacts.

No information is collected as part of this phase of the pilot, nor will any information be collected by employees who use social media for training purposes. Although personally identifiable information may incidentally be visible to CBP personnel during this pilot, the purpose of the initiative is solely to conduct security and infrastructure testing. Neither the testing, nor the use of YouTube for training purposes, is an operational use. Accordingly, this activity does not trigger the DHS or CBP privacy guidance on the use of social media for operational use, and a SMOUT or Rules of Behavior is not currently required.

DHS Privacy agrees with CBP Privacy that this initiative is not privacy sensitive as it does not collect, use, or maintain PII. Accordingly, neither a PIA nor SORN is required. (b) (5) [redacted]

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:

The Privacy Office
U S Department of Homeland Security
Washington, DC 20528
202 (b) (7)(E) @dhs gov
www dhs gov/privacy



# 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.

# 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

a ational use of social media.

u ☐ Rules of Behavior do not comply. <Please explain analysis.>

t ☐ Training required.

h Additional Privacy compliance documentation is required:

o ☒ A PIA is required.

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

i ☐ New.

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

i ☒ A SORN is required:

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

s ☐ New.

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

o

n **DHS PRIVACY OFFICE COMMENTS**

o

t

a

u

t

h

o

r

i

z

e

o

p

e

r

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.

# 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)

**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 criminal 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). 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 OPR JIC and IOD vet the allegations to determine whether any allegation of corruption or misconduct rise to the level of criminal activity. For those allegations determined to be criminal in nature, OPR requires the use of cutting edge investigative methodologies to collect evidence that may be unavailable through traditional investigative means. CBP OPR IOD investigators are aware that targets of criminal investigations may place information, (b) (7)(E) in publicly accessible/non-privacy restricted social media forums. This publicly accessible/non-privacy restricted information has the potential to serve as evidence germane to the criminal activity under investigation. (b) (7)(E) The evidentiary potential of this publicly accessible/non-privacy restricted social media information may be derogatory or mitigating, depending the investigation.

CBP OPR IOD will use social media to gather evidence directly relevant to the criminal activity that predicates their investigations. 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 criminal violations or misconduct. All OPR IOD investigations are predicated on specific allegations or articulable facts that are prima facie indicators of misconduct or criminal violations.

Once an individual is the subject of an investigation, OPR IOD will use social media to gather evidence and relevant information related to the criminal conduct. (b) (7)(E) (b) (7)(E) . 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.

(Note: While some OPR IOD 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 U.S. 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 OPR. Once prosecution of the matter is declined, OPR IOD will conduct any further investigation of the matter pursuant to the Office of Professional Responsibility Administrative Investigation SMOUT.

**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)
- 19 U.S.C. § 1589a, Enforcement authority of customs officers
- 8 U.S.C. § 1357, Powers of immigration officers and employees
- 8 C.F.R. § 287.2, Disposition of criminal cases
- DHS Delegation 7010.3, Delegation of Authority to the Commissioner of U.S. Customs and Border Protection
- Memorandum, Authorization to the Commissioner of CBP to Investigate Allegations of Criminal Misconduct by CBP Employees and to Convert CBP Internal Affairs GS-1801 Employees to GS-1811 Series to Conduct such Investigations (Aug. 29, 2014)
- CBP Directive No. 2130-016, Roles and Responsibilities for Internal Affairs Activities and Functions (December 23, 2008)
- CBP Office of Internal Affairs Order 14-001, Designation Order, Immigration Officer and Customs Officer Authority (Sept. 25, 2014)
- 8 C.F.R. § 2.1, Authority of the Secretary of Homeland Security

(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.**

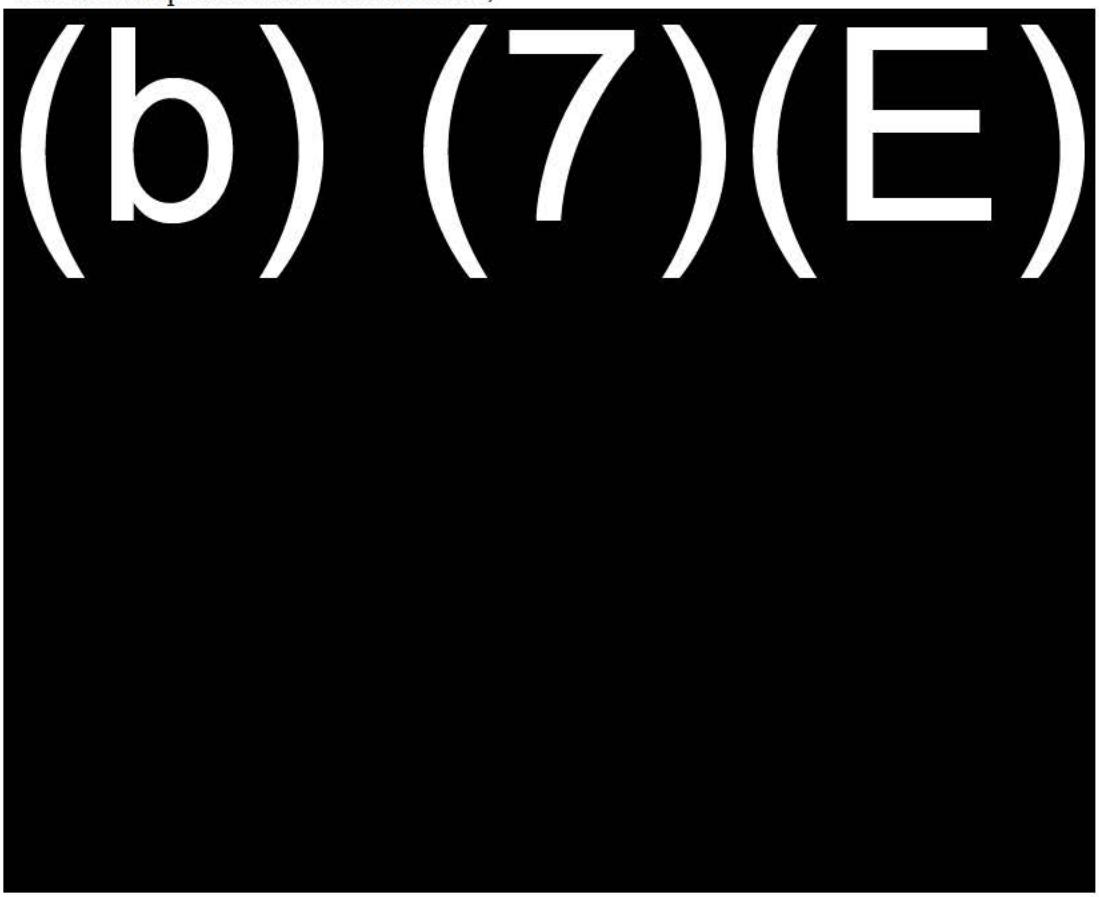
Attached. Also attached is the CBP Directive for Operational Use of Social Media, Section 5

**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;

(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;




**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:

As described in Section 1, all documentation of the operational use of social media for OPR IOD's criminal investigations is done (and stored) within the individual JICMS case file. JICMS has privacy compliance coverage under the DHS/ALL-20- Internal Affairs SORN and the JICMS PIA (DHS/CBP/PIA-044).

**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: 2/21/2018**

**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) Users 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 criminal 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. CBP OPR IOD will use social media to gather evidence directly relevant to the criminal activity that predicates their investigations. 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 criminal violations or misconduct.

(b) (7)(E)

(b) (7)(E) The information is stored in the Joint Integrity Case Management System (JICMS).

While 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. Once prosecution of the matter is declined, OPR IOD will conduct any further investigation of the matter pursuant to the Office of Professional Responsibility Administrative Investigation SMOUT.

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. 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.

# 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)

c. *Public interaction*.

(b) (7)(E)

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.