

# **U.S. CUSTOMS AND BORDER PROTECTION DIRECTIVE**

**CBP DIRECTIVE NO. 5410-003**

**DATE: January 2, 2015**

**ORIGINATING OFFICE: OC-PDO**

**REVIEW DATE: January 2018**

## **SUBJECT: OPERATIONAL USE OF SOCIAL MEDIA**

### **1 PURPOSE**

To assign responsibilities and establish general rules of behavior for the operational uses of social media for U.S. Customs and Border Protection (CBP), in compliance with all applicable statutes, regulations, and Department of Homeland Security (DHS) or government-wide policies.

### **2 SCOPE**

This Directive applies to all CBP employees, contractors, and to persons using CBP systems in furtherance of the CBP mission. However, this Directive does not apply to the operational use of social media for communications and outreach with the public authorized by the DHS Office of Public Affairs. Moreover, this Directive does not apply to the operational use of social media to the extent that CBP is utilizing social media for situational awareness purposes on behalf of the DHS National Operations Center.

### **3 POLICY**

It is the policy of CBP to collect, maintain, use, and disseminate PII through the operational use of social media only when there is an authorized need to know the information. CBP will protect PII collected during the authorized operational use of social media, and comply with DHS privacy policy, applicable privacy laws, federal government-wide policies, and other statutory authorities. The procedures set forth in this directive must be followed before PII may be collected by CBP through the use of social media, stored in a CBP system of records, or shared with another party.

### **4 AUTHORITIES/REFERENCES**

- 4.1 Public Law 107-347, "E-Government Act of 2002," as amended, Section 208 [44 U.S.C. § 3501 note];**
- 4.2 Title 5, U.S. Code, Section 552a, "Records maintained on individuals" [The Privacy Act of 1974, as amended];**
- 4.3 Title 6, U.S. Code, Section 142, "Privacy Officer;"**
- 4.4 Title 8, U.S. Code, Section 1363a;**

FOUO

1

- 4.5 Title 19, U.S. Code, Section 2081;
- 4.6 Title 44, U.S. Code, Chapter 35, Subchapter III, "Information Security" [The Federal Information Security Management Act of 2002, as amended (FISMA)];
- 4.7 Title 6, C.F.R., Chapter 1, Part 5, "Disclosure of records and information;"
- 4.8 DHS Delegation 13001, "Delegation to the Chief Privacy Officer;"
- 4.9 DHS Sensitive Systems Policy Directive 4300A;
- 4.10 DHS Directive 047-01 "Privacy Policy and Compliance" (July 7, 2011) and Instruction 047-01-001 "Privacy Policy and Compliance" (July 25, 2011);
- 4.11 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);
- 4.12 CBP Memorandum "Privacy Compliance and U.S. Customs and Border Protection" (February 10, 2012);
- 4.13 CBP Memorandum "Executive Agent Appointment for a CBP Integrated Intelligence, Surveillance, and Reconnaissance (ISR) Capability" (July 20, 2011);
- 4.14 CBP Information Systems Security Policies and Procedures Handbook 1400-05D; and
- 4.15 CBP Delegation Order 11-001 "Delegation of Authority for Discipline and Adverse Actions" (April 6, 2011).

## 5 DEFINITIONS

- 5.1 ***Business Owner*** means the CBP employee responsible for the planning and operation of a CBP project, operation, or program that collects PII.
- 5.2 ***Fair Information Practice Principles*** means the policy framework adopted by DHS in Directive 047-01, "Privacy Policy and Compliance," regarding the collection, use, maintenance, disclosure, deletion, or destruction of PII.
- 5.3 ***Individual*** means a natural person, including United States citizens and aliens (e.g., lawful permanent residents and nonimmigrants).
- 5.4 ***Masked Monitoring*** means using identities or credentials on social media that do not identify a DHS/CBP affiliation, or otherwise concealing a government affiliation, to conduct research or general, operational awareness. Masked

FOUO

monitoring includes logging in to social media, but does not include engaging or interacting with individuals on or through social media (which is defined as Undercover Engagement, below).

- 5.5 Operational Awareness** means information gathered from a variety of sources that, when communicated to emergency managers and decision makers, can form the basis for incident management or readiness state decision making.
- 5.6 Overt Research** means collecting information from social media without logging in or otherwise interacting with individuals through social media. Overt research does not include creating identities or credentials on social media, nor does it include concealing a government affiliation to conduct research or general, operational awareness (e.g., non-DHS affiliated IP address).
- 5.7 Overt Engagement** means logging in to social media using DHS/CBP-branded credentials or otherwise indicating an official agency presence and engaging or interacting with individuals on or through social media.
- 5.8 Overt Monitoring** means logging in to social media using DHS/CBP-branded credentials or otherwise indicating an official agency presence, but does not include engaging or interacting with individuals on or through social media (which is defined as Overt Engagement, above).
- 5.9 Operational Use** means use of social media to collect PII for the purpose of enhancing general operational awareness, investigating an individual in a criminal, civil, or administrative context, assist in making a benefit determination about a person, assist in making a personnel determination about a CBP employee or contractor, assist in making a suitability determination about a prospective CBP employee or contractor, or for any other official CBP purpose that has the potential to affect the rights, privileges, or benefits of an individual or CBP employee or contractor. Operational use does not include the use of search engines for general Internet research, the use of social media for professional development (e.g., training and continuing education), or the use of social media for facilitating internal meetings, assigning or trading work shifts, or other internal administrative efficiencies.
- 5.10 Personally Identifiable Information (PII)** means any information that permits the identity of an individual to be directly or indirectly inferred, including other information that is linked or linkable to an individual.
- 5.11 Privacy Compliance Documentation** means any document required by statute or by the Chief Privacy Officer that supports compliance with DHS privacy policy, procedures, or requirements, including but not limited to the Social Media Operational Use Template (SMOUT), Privacy Impact Assessments (PIAs), System of Records Notices (SORNs), Notices of Proposed Rulemaking for Exemption from

certain aspects of the Privacy Act (NPRM), and Final Rules for Exemption from certain aspects of the Privacy Act.

- 5.12 *Privacy Liaison*** means the CBP employee responsible for serving as a point of contact and initial identifier of privacy issues in a CBP office.
- 5.13 *Project Manager*** means the CBP employee or contractor in the Office of Information and Technology or other Office responsible for building and technically maintaining an authorized system with privacy implications.
- 5.14 *Social Media*** means the sphere of websites, applications, and web-based tools that connect users to engage in dialogue, share information and media, collaborate, and interact. Social media take many different forms, including but not limited to web-based communities and hosted services, social networking sites, video and photo sharing sites, blogs, virtual worlds, social bookmarking, and other emerging technologies. This definition does not apply to internal Department intranets or applications.
- 5.15 *Social Media Operational Use Template (SMOUT)*** means the document that each office must submit to the CBP Privacy and Diversity Office for approval by the DHS Privacy Office that describes the current or proposed category of operational uses(s) of social media, identifies the appropriate authorities for the current or proposed category of use(s), describes what PII, if any, is or would be collected (and from whom or by what method), how that information is used, where the information would be stored, and if that collection, storage, and usage is consistent with the current SORN, and any appropriate training. The Template is used to identify information technology systems, technologies, rulemakings, programs, or pilot projects that involve collecting PII from social media for the current or proposed category of use(s) and to assess whether there is a need for additional Privacy Compliance Documentation. Through submission to the CBP Privacy and Diversity Office, templates will be reviewed and adjudicated by the DHS Chief Privacy Officer, and every three years thereafter for accuracy.
- 5.16 *System of Records Notice (SORN)*** means the official public notice of a DHS or CBP system of records as required by the Privacy Act of 1974 (as amended). The SORN identifies (1) the purpose for the system of records, (2) the individuals covered by information in the system of records, (3) the categories of records maintained about individuals, (4) the source of the records and (5) the ways in which the information is generally shared by DHS and CBP. The SORN also provides notice of the mechanisms available for individuals to exercise their Privacy Act rights to access and correct the PII that DHS and CBP maintains about them.
- 5.17 *Undercover Engagement*** means using identities or credentials on social media that do not identify a DHS/CBP affiliation, or otherwise concealing a government affiliation, to engage or interact with individuals on or through social media.

FOUO



## **6 RESPONSIBILITIES**

- 6.1 All CBP employees, contractors, and persons using CBP systems in furtherance of the CBP mission are responsible for:**
- 6.1.1 Using social media for operational purposes only when activities are authorized by statute, executive order, regulation, or policy and approved through the procedures in this Directive;**
  - 6.1.2 Using only government-issued equipment, internet connections authorized to access social media through the DHS/CBP network (i.e., no “stand-alone” connections), and government-approved accounts when engaging in the operational use of social media, unless otherwise specifically authorized and approved;**
  - 6.1.3 Use screen names or identities that indicate an official DHS/CBP affiliation and use DHS/CBP email addresses to open accounts used when engaging in the operational use of social media, unless otherwise specifically authorized and approved;**
  - 6.1.4 Accessing publicly available information through social media only by reviewing posted information without interacting with any individual who posted the information, unless otherwise specifically authorized and approved;**
  - 6.1.5 Respecting individuals’ privacy settings and access only information that is publicly available unless the individual whose information the employee seeks to access has given consent to access it, or as otherwise authorized and approved;**
  - 6.1.6 Collecting only the minimum PII necessary for the proper performance of their authorized duties;**
  - 6.1.7 Protecting PII as required by the Privacy Act and DHS privacy policy;**
  - 6.1.8 Documenting operational use of social media, including date, site(s) accessed, information collected, and how it was used in the same manner that CBP would document information collected from any source in the normal course of business;**
  - 6.1.9 Complying with DHS Directive 110-01 and Instructions 110-01-001, with privacy policies and procedures issued by the DHS Chief Privacy Officer, and with applicable CBP policies on operational use of social media; and**
  - 6.1.10 Completing training on the operational use of social media and signing the CBP Operational Use of Social Media Rules of Behavior before any social media use and annually thereafter, if operational use of social media is a continuing requirement in the performance of their responsibilities.**

FOUO

- 6.2 The Assistant Commissioner for the Office of Information and Technology is responsible for:**
- 6.2.1 Providing web technology services, security, and technical assistance for the operational use of social media within CBP; and**
  - 6.2.2 Ensuring that any technical system providing Masked Monitoring and/or Undercover Engagement accurately documents user login credentials and profiles and maintains sufficient audit logs for each user.**
- 6.3 The Assistant Commissioner for the Office of Intelligence and Investigative Liaison is responsible for serving as the Business Owner governing the provision of intelligence, surveillance, and reconnaissance (ISR) capabilities, including Masked Monitoring and Undercover Engagement of Social Media. This includes ensuring Masked Monitoring and Undercover Engagement of Social Media meet operational and intelligence needs and providing direction to Office of Information and Technology (OIT) regarding intelligence related technologies available to be leveraged for all aspects of ISR to be used within CBP.**
- 6.4 The CBP Privacy Officer is responsible for:**
- 6.4.1 Maintaining an accurate accounting of all CBP categories of operational use of social media using the SMOUT to identify collection and use of PII, the authority for such collection and use, and any other attendant privacy impacts, and ensuring CBP implements DHS privacy policy with respect to the operational use of social media;**
  - 6.4.2 Coordinating with CBP Business Owners and Project Managers, as appropriate, together with the DHS Chief Privacy Officer and the Office of Chief Counsel to complete a SMOUT and any other required Privacy Compliance Documentation for (1) for all proposed categories of operational use of social media, and (2) for any changes to the categories of operational use of social media ;**
  - 6.4.3 Developing and reviewing CBP policies and directives related to Operational Use of social media, and CBP Rules of Behavior consistent with the adjudicated Template, to ensure compliance with DHS privacy policy, privacy laws applicable to DHS, and federal government-wide privacy policies;**
  - 6.4.4 Overseeing CBP privacy training for operational use of social media and providing educational materials, consistent with privacy training for operational use of social media developed by the DHS Chief Privacy Officer;**
  - 6.4.5 Reviewing documentation required in 6.1.8 to ascertain compliance with this Directive as needed; and**

FOUO

- 6.4.6 Collaborating with the DHS Chief Privacy Officer in conducting Privacy Compliance Reviews.**
- 6.5 CBP Office of Chief Counsel is responsible for:**
  - 6.5.1 Providing advice to Business Owners or Project Managers, as appropriate, to ensure that appropriate authority exists to engage in categories of operational use of social media before CBP employees engage in those uses, and to ensure that the Template generally documents that authority;**
  - 6.5.2 Providing legal guidance to the CBP Privacy Officer, Business Owners, or Project Managers, as appropriate, in the drafting of CBP Operational Use of Social Media Rules of Behavior Rules of Behavior for operational use of social media.**
- 6.6 CBP Business Owners and Project Managers, as appropriate, are responsible for:**
  - 6.6.1 Coordinating with the CBP Privacy Officer to ensure that privacy is appropriately addressed when proposing, developing, implementing, or changing any operational use of social media;**
  - 6.6.2 Coordinating with the CBP Privacy Officer and the Office of Chief Counsel to prepare draft Templates and CBP Operational Use of Social Media Rules of Behavior, and, as appropriate, all Privacy Compliance Documentation required when proposing, developing, or implementing or changing any category of operational use of social media;**
  - 6.6.3 Monitoring the design, deployment, operation, and retirement of programs involving the operational use of social media to ensure that the use of PII, if any, is limited to those uses described in the Privacy Compliance Documentation;**
  - 6.6.4 Ensuring oversight mechanisms, including, for example, audit trails and/or privacy compliance reviews, as appropriate, are built into the design of programs and systems involving the operational use of social media;**
  - 6.6.5 Coordinating with the CBP Privacy Officer to establish administrative, technical, and physical controls for storing and safeguarding PII consistent with DHS privacy, security, and records management requirements to ensure the protection of PII from unauthorized access, disclosure, or destruction in the course of operational use of social media; and**
  - 6.6.6 Supporting the CBP Privacy Officer in developing and implementing privacy procedures and job-related privacy training to safeguard PII in operational uses of social media.**

FOUO

**6.7 Supervisors are responsible for:**

**6.7.1** Reviewing request(s) for Overt Research of social media, considering the purpose of the request, and determining whether granting approval would serve an appropriate authorized purpose for an operational need that has been approved by the Chief Privacy Officer through a SMOUT; and

**6.7.2** Approving or denying such requests.

**6.8 Second Level Supervisors, or higher, are responsible for:**

**6.8.1** Reviewing request(s) for Overt Monitoring, Overt Engagement, and Masked Monitoring of social media, considering the purpose of the request, and determining whether granting approval would serve an appropriate authorized purpose for an operational need that has been approved by the Chief Privacy Officer through a SMOUT; and

**6.8.2** Approving or denying such requests.

**6.9 Supervisors in the Senior Executive Service, and Second Level Supervisors at the GS-15 Level, or higher, delegated by the Office of Internal Affairs Director of Investigative Operations Division are responsible for:**

**6.9.1** Reviewing request(s) for Undercover Engagement of social media, considering the purpose of the request, and determining whether granting approval would serve an appropriate authorized purpose for an operational need that has been approved by the Chief Privacy Officer through a Template; and

**6.9.2** Approving or denying such requests.

**7 PROCEDURES**

**7.1 General Procedures**

**7.1.1** Each CBP Office must complete a Template. That Template must identify which parts of the Office engages in operational use of social media, the type of operational use and the purposes achieved through the program(s). This must be completed before engaging in any operational uses of social media, including Overt Research, Overt Monitoring, Overt Engagement, Masked Monitoring, or Undercover Engagement.

**7.1.2** The Office must provide the completed Template to the CBP Privacy and Diversity Office via its Privacy Liaison (if the office has a designated Privacy Liaison) or directly to the CBP Privacy Officer.

- 7.1.3** The CBP Privacy and Diversity Office, with appropriate coordination with the Office of Chief Counsel, must review and approve the Template before submitting it to the DHS Chief Privacy Officer for review and approval.
- 7.1.4** If directed by the DHS Chief Privacy Officer, the CBP Privacy Officer and the Office must complete any Privacy Compliance Documentation to address the particular operational use of social media stated in the completed Template.
- 7.1.5** The Office must complete any other additional steps outlined in Sections 7.2, 7.3, 7.4, 7.5, or 7.6 of this Directive, as appropriate.
- 7.1.6** Authorized CBP employees, contractors, and persons using CBP systems in furtherance of the CBP mission who plan to use social media under this directive, after a Template is approved, must complete training regarding the Operational Use of social media. These persons must also sign and comply with the CBP Operational Use of Social Media Rules of Behavior before engaging in any of the activities listed in Sections 7.2, 7.3, 7.4, 7.5, or 7.6 of this Directive, and annually thereafter.
- 7.1.7** All CBP employees, contractors, and persons using CBP systems in furtherance of the CBP mission who have created and used social media log-in credentials or profiles for operational use prior to the promulgation of this Directive must submit a request as specified in Sections 7.2, 7.3, 7.4, 7.5, or 7.6 of this Directive and must also complete training and sign the CBP Operational Use of Social Media Rules of Behavior within 90 days of the implementation date of this Directive to continue utilizing the credential or profile.
- 7.1.8** All information collected through social media must be recorded in the appropriate system of records, including date, site(s) accessed, information collected, and how the information was used, in the same manner that CBP would document information collected from any source in the normal course of business. All information collected through social media must be protected in the appropriate system of records to the same extent as other PII in that system and follow any chain of custody requirements for that system, as appropriate.

## **7.2 Overt Research**

- 7.2.1** CBP employees, contractors, and persons using CBP systems in furtherance of the CBP mission must obtain approval from a CBP supervisor before conducting Overt Research of social media.
- 7.2.2** CBP employees, contractors, and persons using CBP systems in furtherance of the CBP mission may conduct Overt Research of social media, after obtaining approval, if the research is necessary for an authorized purpose with a clear nexus to their assigned duties after a properly approved Template is in place.



### **7.3 Overt Monitoring of Social Media**

- 7.3.1** CBP employees, contractors, and persons using CBP systems in furtherance of the CBP mission must obtain approval from a second level CBP supervisor, or higher, before Overt Monitoring of social media.
- 7.3.2** Requests for approval for Overt Monitoring of social media must describe the authorized mission, the CBP employees, contractors, and persons using CBP systems in furtherance of the CBP mission authorized to use social media, the nexus to their assigned duties, the social media and any log-in credentials and profile information (including names, email addresses, photographs, etc.) used, and the authority to conduct the program.
- 7.3.3** Approved employees, contractors, and persons using CBP systems in furtherance of the CBP mission must identify themselves as associated with CBP by applying appropriate branding and disclaimers to distinguish the agency's activities from those of nongovernment actors. For example, Business Owners or Project Managers should add the CBP seal or emblem to the program's profile page on a social media website to indicate that it is an official agency presence.

### **7.4 Overt Engagement of Social Media**

- 7.4.1** CBP employees, contractors, and persons using CBP systems in furtherance of the CBP mission must obtain approval from a second level CBP supervisor, or higher, before Overt Engagement of social media.
- 7.4.2** Requests for approval for Overt Engagement of social media must describe the authorized mission, the CBP employees contractors, and persons using CBP systems in furtherance of the CBP mission authorized to use social media, the nexus to their assigned duties, the social media and any log-in credentials and profile information (including names, email addresses, photographs, etc.) used, and the authority to conduct the program.
- 7.4.3** Approved employees, contractors, and persons using CBP systems in furtherance of the CBP mission must identify themselves as associated with CBP by applying appropriate branding and disclaimers to distinguish the agency's activities from those of nongovernment actors. For example, Business Owners or Project Managers should add the CBP seal or emblem to the program's profile page on a social media website to indicate that it is an official agency presence.

### **7.5 Masked Monitoring**

- 7.5.1** (b) (7)(E)





7.5.2 Approval of Masked Monitoring of social media must be re-approved every (b) (7) (E)

7.5.3 (b) (7)(E)

7.5.4 Requests for Approval for Masked Monitoring of social media must describe the authorized purpose for an operational need, the CBP employees, contractors, and persons using CBP systems in furtherance of the CBP mission authorized to conduct the Masked Monitoring of social media, the nexus to their assigned duties, the social media sites to be accessed, log-in credentials and profile information (including names, email addresses, photographs, etc.) used, and the authority to conduct the program. (b) (7)(E)

7.5.5 Approved employees, contractors, and persons using CBP systems in furtherance of the CBP mission must comply with the specific terms for "Undercover Operational Use of Social Media and the Public Internet" as set forth in the attached CBP Operational Use of Social Media Rules of Behavior.

## 7.6 Undercover Engagement of Social Media

7.6.1 CBP employees, contractors, and persons using CBP systems in furtherance of the CBP mission may obtain approval to use social media for Undercover Engagement only when necessary for authorized law enforcement purposes with a clear nexus to their assigned duties and in conformance with existing undercover operations policies.

7.6.2 (b) (7)(E)

7.6.3 (b) (7)(E)

7.6.4 Approval of Undercover Engagement of Social Media must be re-approved every (b) (7)(E) through the procedures in 7.6.2.

7.6.5 Requests for Approval for Undercover Engagement of Social Media must describe the authorized purpose for an operational need, the CBP employees, contractors, and to persons using CBP systems in furtherance of the CBP mission authorized to use social media under cover, the social media sites used, log-in credentials and profile information (including names, email addresses, photographs, etc.) used, and the authority to conduct the program. (b) (7)(E)

(b) (7)(E)

- 7.6.6 Approved employees, contractors, and to persons using CBP systems in furtherance of the CBP mission must comply with the specific terms for "Under cover Operational Use of Social Media and the Public Internet" as set forth in the attached CBP Operational Use of Social Media Rules of Behavior.

## **8 PRIVACY INCIDENT HANDLING**

- 8.1 Unauthorized use of social media will be considered a Privacy Incident.
- 8.2 In accordance with the DHS Privacy Incident Handling Guidance, all Privacy Incidents are to be immediately reported, as appropriate, to the DHS Security Operations Center (SOC) or CBP Computer Security Incident and Response Center (CSIRC) for review, investigation, mitigation, and remediation, as necessary.
- 8.3 Pursuant to CBP Delegation Order 11-001 "Delegation of Authority for Discipline and Adverse Actions" (April 6, 2011), unauthorized use of social media may be grounds for appropriate disciplinary action, as determined by the employee's supervisor.

## **9 MEASUREMENT/INSPECTION**

- 9.1 CBP's Office of Internal Affairs, Management Inspections Division, shall develop and periodically, or at a minimum once each calendar year, administer an inspection mechanism to determine whether CBP Offices are in full compliance with this Directive.

## **10 DISCLOSURE**

- 10.1 This Directive is for internal use only and may not be shared with the public.

## **11 NO PRIVATE RIGHT CREATED**

This document is for internal CBP use only, and does not create or confer any rights, privileges, or benefits for any person or entity.

(b) (6), (b) (7)(C)

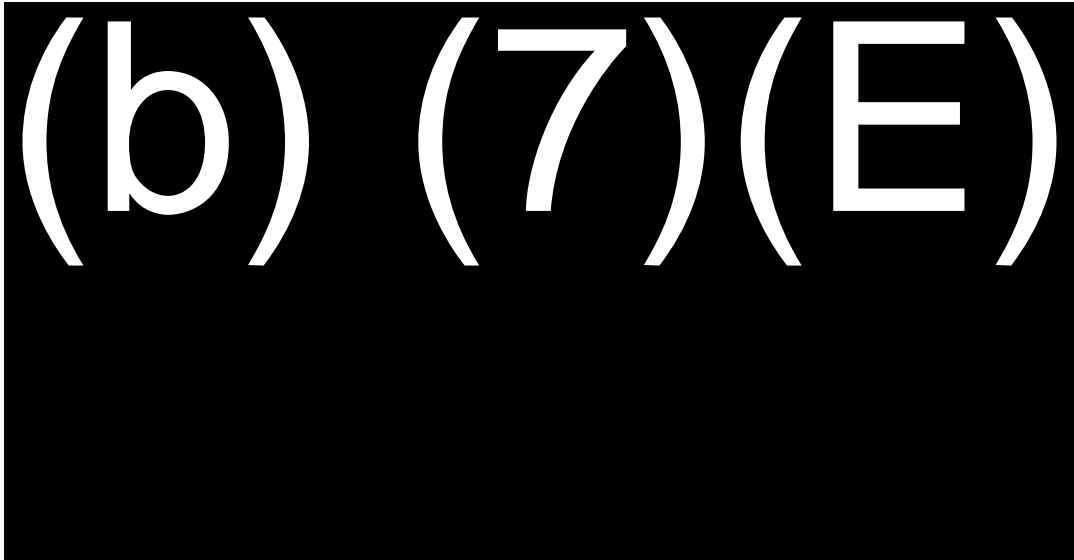
Commissioner  
U.S. Customs and Border Protection

## U.S. Customs and Border Protection

### Interim Standard Operating Procedure for CBP Access to Operational Use of Social Media

- I. **Purpose:** This Interim Standard Operating Procedure (SOP) for CBP Access to Operational Use of Social Media establishes the implementation process for U.S. Customs and Border Protection (CBP) employees and contractors to access social media for operational purposes. Implementation will occur through coordination between the Privacy and Diversity Office and Office of Information and Technology.
- II. **Authorities/References:**
- a. DHS Directive 047-01, "Privacy Policy and Compliance" (July 7, 2011)
  - b. DHS Instruction 047-01-001, "Privacy Policy and Compliance" (July 25, 2011)
  - c. DHS Directive 110-01, "Privacy Policy for Operational Use of Social Media" (June 8, 2012)
  - d. CBP Directive 2120-010, "Privacy Policy, Compliance, and Implementation" (January 2, 2015)
  - e. CBP Directive 5410-003, "Operational Use of Social Media" (January 2, 2015)
  - f. Memorandum from the Deputy Secretary to Component Heads, "Designation of Component Privacy Officers" (June 5, 2009)
- III. **Definitions:**

a.



- b. *Masked Monitoring* means using identities or credentials on social media that do not identify a DHS/CBP affiliation, or otherwise concealing a government affiliation to conduct research or general, operational awareness. Masked monitoring includes logging in to social media, but does not include engaging or

interacting with individuals on or through social media (which is defined as Undercover Engagement).

- c. *Operational Awareness* means information gathered from a variety of sources, that when communicated to emergency managers and decision makers, can form the basis for incident management or readiness state decision making.
- d. *Operational Use* means use of social media to collect personally identifiable information (PII) for the purpose of enhancing general operational awareness, investigating an individual in a criminal, civil, or administrative context, assist in making a benefit determination about a person, assist in making a personnel determination about a CBP employee or contractor, assist in making a suitability determination about a prospective CBP employee or contractor, or for any other official CBP purpose that has the potential to affect the rights, privileges, or benefits of an individual or CBP employee or contractor. Operational use does not include the use of search engines for general Internet research, the use of social media for professional development (e.g., training and continuing education), or the use of social media for facilitating internal meetings, assigning or trading work shifts, or other internal administrative efficiencies.
- e. *Overt Research* means collecting information from social media without logging in or otherwise interacting with individuals through social media. Overt research does not include creating identities or credentials on social media, nor does it include concealing a government affiliation to conduct research or general, operational awareness (e.g., non-DHS affiliated IP address).
- f. *Overt Engagement* means logging in to social media using DHS/CBP-branded credentials or otherwise indicating an official agency presence and engaging or interacting with individuals on or through social media.
- g. *Overt Monitoring* means logging in to social media using DHS/CBP-branded credentials or otherwise indicating an official agency presence, but does not include engaging or interacting with individuals on or through social media (which is defined as Overt Engagement).
- h. *Personally Identifiable Information (PII)* means any information that permits the identity of an individual to be directly or indirectly inferred, including other information that is linked or linkable to an individual.
- i. *Social Media* means the sphere of websites, applications, and web-based tools that connect users to engage in dialogue, share information and media, collaborate, and interact. Social media takes many different forms, including but not limited to web-based communities and hosted services, social networking sites, video and photo sharing sites, blogs, virtual worlds, social bookmarking, and other emerging technologies. This definition does not apply to internal Department intranets or applications.



- j. *Social Media Operational Use Template (SMOUT)* means the document that each office must submit to CBP Privacy Office for approval by the DHS Privacy Office that describes the current or proposed category of operational use(s) of social media, identifies the appropriate authorities for the current or proposed category of use(s), describes what PII, if any, is or would be collected (and from whom or by what method), how that information is used, where the information would be stored, and if that collection, storage, and usage is consistent with the current SORN, and any appropriate training. The SMOUT is used to identify information technology systems, technologies, rulemaking, programs, or pilot projects that involve collecting PII from social media for the current or proposed category of use(s) and to assess whether there is a need for additional Privacy Compliance Documentation. Through submission to the CBP Privacy Office, templates will be reviewed and adjudicated by the DHS Chief Privacy Officer, and every three years thereafter for accuracy.
- k. *Undercover Engagement* means using identities or credentials on social media that do not identify a DHS/CBP affiliation, or otherwise concealing a government affiliation, to engage or interact with individuals on or through social media.

**IV. Procedures:**

- a. A CBP employee completes an online application through the (b) (7)(E) (b) (7)(E) (b) (7)(E) requesting access to social media using the (b) (7)(E) (b) (7)(E) form. Information in the online application must include a detailed business justification as to why the employee needs access to social media through (b) (7)(E).
- b. After review of the (b) (7)(E) application, the CBP Office of Information and Technology, Security Operations Center (CBP SOC), forwards information from the (b) (7)(E) name of employee, phone number, email address, location, supervisor information, and business justification, to the CBP Privacy Office's email address (b) (7)(E) for review and CBP Privacy Officer approval.
- c. The CBP Privacy Officer and/or designee verifies that the individual has completed the mandatory training and signed the CBP Operational Use of Social Media Rules of Behavior, and reviews the provided business justification to determine if it is appropriate for the requested use and is authorized by an approved Social Media Operational Use Template (SMOUT).

The determination made by the CBP Privacy Office and provided to CBP SOC will be one of the following:

- (i) *Approved*: all required training has been completed, a copy of the signed Rules of Behavior has been provided to CBP Privacy, and the business

justification is in accordance with assigned job duties and authorized by an approved SMOUT.

- (ii) *Additional information required:* employee has either not completed training or signed the Rules of Behavior (or both), or additional information is needed regarding the business justification.
  - (iii) *Disapproved:* the business justification is not in accordance with assigned job duties and/or an approved SMOUT.
- d. After receipt of the CBP Privacy Office's determination, the CBP SOC forwards the application to CBP Office of Information and Technology, Chief Information Security Officer (CISO), for further review.

The CISO verifies approval of the individual's request with the employee's Supervisor based on the type of use as outlined by the requirements described below and responds to CBP SOC with either an approval or disapproval:

- i. First Line Supervisors:
    - a. Review requests for Overt Research use of social media, considers the purpose of the requests, and determines whether granting approval would serve an appropriate authorized purpose for an operational need; and
    - b. Approve or deny the requests.
  - ii. Second Level Supervisors, or higher:
    - a. Review requests for Overt Monitoring, Overt Engagement, and Masked Monitoring use of social media, considers the purpose of the request, and determines whether granting approval would serve an appropriate authorized purpose for an operational need; and
    - b. Approve or deny the requests.
  - iii. Supervisors in the Senior Executive Service, and Second Level Supervisors at the GS-15 Level, or higher, delegated by the Office of Internal Affairs Director of Investigations Division:
    - a. Review requests for Undercover Engagement use of social media, considers the purpose of the request, and determines whether granting approval would serve an appropriate authorized purpose for an operational need; and
    - b. Approve or deny the requests.
- e. After receipt of the CISO's review and response (approval or disapproval), CBP SOC forwards the (b) (7)(E) to the DHS SOC for final approval and implementation of access to the (b) (7)(E)
- f. After implementation by the DHS SOC, CBP SOC forwards the (b) (7)(E) number and date of implementation to the CBP Privacy Office for accounting purposes.



Interim SOP for CBP Access to Social Media  
FOUO

- V. **Questions:** Questions concerning this SOP may be directed to the CBP Privacy and Diversity Office at [REDACTED] (b) (7)(E)

U.S. Customs and Border Protection

Privacy and Diversity Office

[REDACTED] (b) (6), (b) (7)(C)

[REDACTED] (b) (6), (b) (7), CBP Privacy Officer

U.S. Customs and Border Protection

Office of Information and Technology

[REDACTED] (b) (6), (b) (7)(C)

Phil Landfried, Deputy Assistant Commissioner



**U.S. Customs and  
Border Protection**

**FEB 15 2018**

MEMORANDUM FOR: Investigative Operations Division (IOD)  
FROM: (b) (6), (b) (7)(C) (b) (6), (b) (7)(C)  
Executive Director  
Investigative Operations Division  
SUBJECT: Operational Use of Social Media for IOD

The purpose of this memorandum is to provide guidance to the IOD SAC Offices when IOD Special Agents use social media during the course of an investigation.

Effective February 12, 2018, DHS approved IOD's documentation which permits the use of social media in criminal and administrative investigations. All agents must read, acknowledge, and comply with the requirements in this memorandum, as well as, applicable DHS and CBP operational use of social media directives and Rules of Behavior. All agents must sign the attached Operational Use of Social Media for IOD Acknowledgement of Receipt. All agents must be mindful that pursuant to CBP Directive 1440-026A, Reporting Allegations of Misconduct dated April 17, 2017, or any superseding CBP Directive, any violation of a CBP Directive or policy shall be immediately documented and reported to the JIC.

**Operational Use of Social Media Investigations**

**General**

OPR IOD may use social media during the course of both criminal and administrative investigations. It is incumbent upon each SA to understand the below governing documents and comply when using social media for operational purposes. Direct any questions regarding the use of social media to an OPR IOD Headquarters Director.

SAs will conduct all social media investigations in accordance with the [CBP Operational Use of Social Media Directive 5410-003](#), the CBP Operational Use of Social Media Rules of Behavior, the [DHS Directive 110-01-001 "Privacy Policy for Operational Use of Social Media"](#), the approved IOD Criminal Investigations Social Media Operational Use Template, and the approved IOD Administrative Social Media Operational Use Template.

## Approval Process

**Special Agents:** Prior to using social media during the course of an investigation, SAs must complete the training on the [Operational Use of Social Media](#), located on Sharepoint. SAs must read and understand the IOP, the CBP Operational Use of Social Media Directive 5410-003, the CBP Operational Use of Social Media Rules of Behavior, and DHS Directive 110-01-001 "Privacy Policy for Operational Use of Social Media. Signed acknowledgements for the training and Operational Use of Social Media Rules of Behavior are kept in the SA's local personnel file, as well as forwarded to the CBP Privacy Office at (b) (7)(E)

Lastly, SAs must submit a request for approval online via (b) (7)(E). The online approval request shall be submitted every six months. The signed acknowledgements for the training and Operational Use of Social Media Rules of Behavior must be submitted annually after initial approval is received.

**First Level Supervisors:** Review requests for (b) (7)(E) of Social Media. Consider the purpose of the request and determine whether approval would serve an appropriate authorized purpose for an operational need that has been approved by the DHS Privacy Office through a Social Media Operational Use Template (SMOUT) and approve or deny such requests.

**Second Level Supervisors or Higher:** Review requests for (b) (7)(E) of social media. Consider the purpose of the request and determine whether granting approval would serve an appropriate authorized purpose for an operational need that has been approved by the DHS Privacy Office through a SMOUT and approve or deny such requests.

## Documentation

All information collected through social media must be recorded in the appropriate system of record. In the case of OPR IOD, JICMS is the appropriate system of record. The information obtained must be documented in an ROI for each operational use of social media. Each ROI must contain the following information:

- (b) (7)(E)
- (b) (7)(E)
- (b) (7)(E)
- (b) (7)(E)

All information collected through social media must be protected to the same extent as other PII in JICMS and must follow any chain of custody requirements for that system, as appropriate.

## Types of Operational Use

IOD SMOUTS are approved for use in criminal and administrative investigations. SAs are permitted to use (b) (7)(E) techniques in relation to Social Media investigations.



(b) (7)(E)

CBP employees, contractors, and persons using CBP systems in furtherance of the CBP mission may conduct (b) (7)(E) of social media, after obtaining approval, if the research is necessary for an authorized purpose with a clear nexus to their assigned duties after a properly approved Template is in place.

(b) (7)(E)

(b) (7)(E)

**PROHIBITED SOCIAL MEDIA ENGAGEMENT BY SAs**

OPR IOD does not (b) (7)(E) and is not able to conduct (b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)



Approved IOD employees using the CBP systems in furtherance of the CBP mission must comply with the specific terms for (b) (7)(E)

(b) (7)(E) as set forth in the CBP Operational Use of Social Media Rules of Behavior.

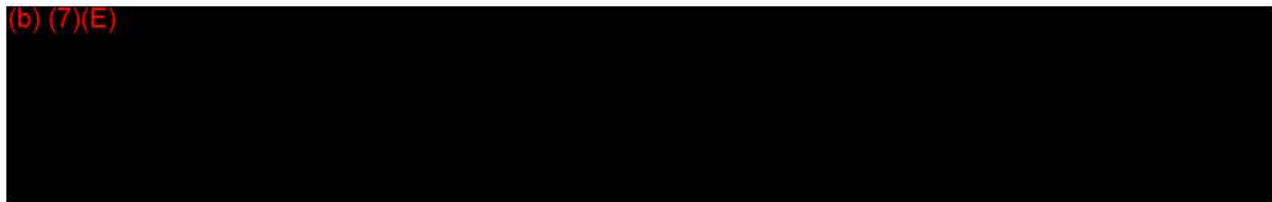
(b) (7)(E)



(b) (7)(E)

This requires approval from a second level supervisor or higher.

(b) (7)(E)



Approved employees, contractors, and persons using CBP systems in furtherance of the CBP mission must identify themselves as associated with CBP by applying appropriate branding and disclaimers to distinguish the agency's activities from those of nongovernment actors. For example, Business Owners or Project Managers should add the CBP seal or emblem to the program's profile page on a social media website to indicate that it is an official agency presence.

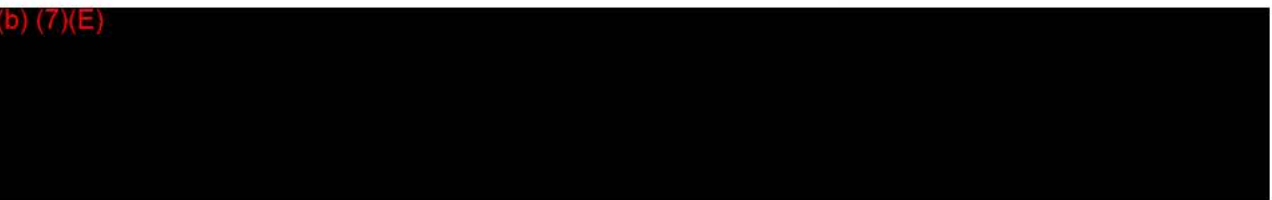
(b) (7)(E)



(b) (7)(E)

This requires approval from a second level supervisor or higher.

(b) (7)(E)



Approved employees, contractors, and persons using CBP systems in furtherance of the CBP mission must identify themselves as associated with CBP by applying appropriate branding and disclaimers to distinguish the agency's activities from those of nongovernment actors. For example, Business Owners or Project Managers should add the CBP seal or emblem to the program's profile page on a social media website to indicate that it is an official agency presence.

U.S. Customs & Border Protection  
Office of Professional Responsibility  
Investigative Operations Division

**Operational Use of Social Media for IOD  
Acknowledgement of Receipt**

As a CBP Special Agent/Investigator who is authorized to carry out the investigative functions of the Office of Professional Responsibility, you are required to comply with and be thoroughly familiar with all aspects of the attached IOD memorandum on Operational Use of Social Media for IOD.

You have been provided a complete copy of the *IOD* memorandum on Operational Use of Social Media for IOD and the opportunity to discuss the contents with your supervisor or other management officials.

By signing this statement, you acknowledge that you have read, understand, and agree to comply with all parts and aspects of the *IOD* memorandum on Operational Use of Social Media for IOD.

\_\_\_\_\_  
Employee's Name (Printed)

\_\_\_\_\_  
Employee's Signature

\_\_\_\_\_  
Date

\_\_\_\_\_  
Employee's Duty Location

\_\_\_\_\_  
Supervisor's Name (Printed)

\_\_\_\_\_  
Supervisor's Signature

\_\_\_\_\_  
Date

This signed acknowledgment shall be included in the employee's local personnel file, subject to IOD Inspection Program review. The acknowledgement form shall also be forwarded by the supervisor to (b) (7)(E) \_\_\_\_\_.



(b) (6), (b) (7)(C)

---

**From:** (b) (6), (b) (7)(C)  
**Sent:** Wednesday, March 27, 2019 11:15 AM  
**To:** (b) (6), (b) (7)(C)  
**Cc:**  
**Subject:** Re: Question-DHS/CBP Privacy Assessment

Thank you (b) (6), (b) (7)(C) for the quick follow up.

Hi (b) (6), (b) (7)(C)

Our concern is we receive quite a bit of outreach from governments, advocacy groups, and our users about our companies doing more to stop the fraudulent account creation by scammers and terrorist groups... As such, the creation of fake profiles by any sector, including law enforcement, violates our standards.

When possible, we would like to speak to you and the team about our concerns and also hear your perspectives.

Best,

(b) (6), (b) (7)(C)

Sent from my iPhone

On Mar 27, 2019, at 10:49 AM, (b) (6), (b) (7)(C) <[@hq.dhs.gov](mailto:(b) (6), (b) (7)(C)@hq.dhs.gov)> wrote:

Hi (b) (6), (b) (7)(C)

-- Thanks for reaching out. This was a privacy impact assessment of an existing policy regarding the review of publicly available information on platforms, not new policy or an expansion of existing policy. PIAs are required at regular intervals.

For further context from the PIA: "If necessary, CBP may create accounts on social media sites in order to view publicly available information. CBP employees then review the posts captured by the monitoring tools in order to determine whether they are relevant for situational awareness and threat monitoring.

CBP is permitted by policy to establish user names and passwords to create profiles and follow relevant government, media, and subject matter experts on social media sites in order to use search tools under established criteria and search terms for monitoring that supports providing situational awareness."

I'm connecting you here with (b) (6), (b) (7)(C) at CBP who can answer additional questions.

Thanks,

(b) (6), (b) (7)(C)

(b) (6), (b) (7)(C)

Director, Cybersecurity and Innovation

DHS Private Sector Office

(b) (6), (b) (7)(C)

**From:** (b) (6), (b) (7)(C)  
**Sent:** Tuesday, March 26, 2019 6:48:16 PM  
**To:** (b) (6), (b) (7)(C)  
**Subject:** Question-DHS/CBP Privacy Assessment

Hi (b) (6), (b) (7)(C)

We noticed [this doc](#) posted on a DHS website today describing how Customs and Border Protection is now expanding its use of social media platforms:

*“If necessary, CBP may create accounts on social media sites in order to view publicly available information...”*

*“Some CBP personnel, consistent with CBP policy and procedures,20 may conceal their identity when viewing social media for operational security purposes...”*

Would you provide additional context on this policy?

Best,

(b) (6), (b) (7)(C)



## **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: 202-343-1717

PIA@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](http://www.dhs.gov/privacy), on DHS Connect and directly from the DHS Privacy Office via email: [pia@hq.dhs.gov](mailto:pia@hq.dhs.gov), phone: 202-343-1717.



## PRIVACY THRESHOLD ANALYSIS (PTA)

### SUMMARY INFORMATION

<b>Project or Program Name:</b>	<b>(b) (7)(E)</b>		
<b>Component:</b>	Customs and Border Protection (CBP)	<b>Office or Program:</b>	<b>Office of Intelligence and The Office of Professional Responsibility</b>
<b>Xacta FISMA Name (if applicable):</b>	N/A	<b>Xacta FISMA Number (if applicable):</b>	N/A
<b>Type of Project or Program:</b>	<b>Program</b>	<b>Project or program status:</b>	<b>Operational</b>
<b>Date first developed:</b>	<b>March 12, 2018</b>	<b>Pilot launch date:</b>	<b>March 12, 2018</b>
<b>Date of last PTA update</b>	<b>March 12, 2018</b>	<b>Pilot end date:</b>	<b>May 31, 2018</b>
<b>ATO Status (if applicable)</b>	<b>Not started</b>	<b>ATO expiration date (if applicable):</b>	Click here to enter a date.

### PROJECT OR PROGRAM MANAGER

<b>Name:</b>	<b>(b) (6), (b) (7)(C)</b>		
<b>Office:</b>	<b>Office of Intelligence</b>	<b>Title:</b>	Program Manager
<b>Phone:</b>	<b>(b) (6), (b) (7)(C)</b>	<b>Email:</b>	<b>(b) (6), (b) (7)(C)</b>

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

<b>Name:</b>	Click here to enter text.		
<b>Phone:</b>	Click here to enter text.	<b>Email:</b>	Click here to enter text.

### Specific PTA Questions

<b>1. Reason for submitting the PTA: New PTA</b>
--





This PTA provides an overview of CBP's (b) (7)(E) is a collaborative effort between CBP's Office of Intelligence (OI) and the Office of Professional Responsibility (OPR) to identify (b) (7)(E) to CBP personnel. (b) (7)(E)

(b) (7)(E)

OI's (b) (7)(E) through the collection of open source information and collaboration with other law enforcement and government partners, is designed to (b) (7)(E)

(b) (7)(E)

Partners include, but are not limited to the United States Marshal Service, other Department of Homeland Security components, The Federal Bureau of Investigation, State and Local Law Enforcement, the Intelligence Community and the Interagency. In order to (b) (7)(E) require the collection of Personally Identifiable Information (PII). The collection of PII will be limited to individuals (b) (7)(E)

(b) (7)(E) will collect PII through social media posts made in public forums, reports from concerned citizens, media reporting, and may receive (b) (7)(E)

(b) (7)(E). Information acquired will be evaluated by CBP personnel (b) (7)(E)

(b) (7)(E)

No PII, including but not limited to screennames, social media handles, and IP address will be retained unless it is in support of (b) (7)(E) Under this effort, CBP elements supporting (b) (7)(E) will provide the information to both OPR, and OI, who will coordinate its upload into the (b) (7)(E)

(b) (7)(E) CBP necessarily collects information on individuals who, upon further investigation, do (b) (7)(E) to CBP employees or assets. In such cases, (b) (7)(E) will take no further action, but may continue to retain the information as necessary (b) (7)(E)

Additionally, (b) (7)(E) will not report on First Amendment protected speech or activities, however, if such activities (b) (7)(E) a report will be generated and sent to the (b) (7)(E) All personnel supporting this effort are trained law enforcement officers/agents, intelligence specialist and are familiar with the protections afforded under the law and the 1<sup>st</sup> Amendment. (b) (5)



(b) (5) [redacted] (b) (7)(E) will be augmented with personnel specifically trained to access, use, and protect PII when accessing social media (b) (7)(E) personnel will respect privacy settings on all platforms, and will only access publicly available information.

<p><b>2. Does this system employ any of the following technologies:</b> <i>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.</i></p>	<p><input type="checkbox"/> Closed Circuit Television (CCTV)</p> <p><input checked="" type="checkbox"/> Social Media</p> <p><input type="checkbox"/> Web portal<sup>1</sup> (e.g., SharePoint)</p> <p><input type="checkbox"/> Contact Lists</p> <p><input type="checkbox"/> None of these</p>
--	--

<p><b>3. From whom does the Project or Program collect, maintain, use, or disseminate information?</b> <i>Please check all that apply.</i></p>	<p><input type="checkbox"/> This program does not collect any personally identifiable information<sup>2</sup></p> <p><input checked="" type="checkbox"/> Members of the public</p> <p><input checked="" type="checkbox"/> DHS employees/contractors (list components):</p> <p><input type="checkbox"/> Contractors working on behalf of DHS</p> <p><input type="checkbox"/> Employees of other federal agencies</p>
--	---

<p><b>4. What specific information about individuals is collected, generated or retained?</b></p>	
<p>a.</p> <p>b.</p>	<p>(b) (7)(E)</p>

<sup>1</sup> 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.

<sup>2</sup> 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.





c.	(b) (7)(E)
d.	
e.	

<p><b>4(a) Does the project, program, or system retrieve information by personal identifier?</b></p>	<p><input type="checkbox"/> No. Please continue to next question.  <input checked="" type="checkbox"/> Yes. If yes, please list all personal identifiers used: include but not limited to:</p> <div style="background-color: black; color: white; text-align: center; padding: 5px; font-size: 24px;">(b) (7)(E)</div>
--	--



	<b>(b) (7)(E)</b>
<b>4(b) Does the project, program, or system use Social Security Numbers (SSN)?</b>	<input type="checkbox"/> No. <input checked="" type="checkbox"/> Yes. Entered as a case file within <span style="background-color: black; color: white;">(b)(7)(E)</span> or received as part of existing partner agency case file
<b>4(c) If yes, please provide the specific legal basis and purpose for the collection of SSNs:</b>	Collection will be used for identity verification as part of a CBP <span style="background-color: black; color: white;">(b) (7)(E)</span> or received as part of a partner agency case file. Authorities are outlined in CBP Directive No. 5410-003; CBP Directive 1440-027 Security Liaison Program; Participation under CBP Directive 4220-003A- Program for Fugitives wanted by U.S Customs; Title 18, Section 111, Assaulting, Resisting, or Impeding Certain Officers or Employees, and Section 1114, Protection of Officers and Employees of the United States; Executive Order 9397..
<b>4(d) If yes, please describe the uses of the SSNs within the project, program, or system:</b>	Identity verification.
<b>4(e) If this project, program, or system is an information technology/system, does it relate solely to infrastructure?</b>	<input checked="" type="checkbox"/> No. Please continue to next question. <input type="checkbox"/> Yes. If a log kept of communication traffic, please answer the following question.



<i>For example, is the system a Local Area Network (LAN) or Wide Area Network (WAN)?</i>	
<b>4(f) If header or payload data<sup>3</sup> is stored in the communication traffic log, please detail the data elements stored.</b>	
Click here to enter text.	

<b>5. Does this project, program, or system connect, receive, or share PII with any other DHS programs or systems<sup>4</sup>?</b>	<input type="checkbox"/> No. <input checked="" type="checkbox"/> Yes. If yes, please list: (b) (7)(E) (b) (7)(E)
<b>6. Does this project, program, or system connect, receive, or share PII with any external (non-DHS) partners or systems?</b>	<input type="checkbox"/> No. <input checked="" type="checkbox"/> Yes. If yes, please list: Federal, State, Local Government & Law Enforcement Agencies. Foreign Government Law Enforcement Partners (b) (7)(E) comes from outside of the Continental United States.
<b>6(a) Is this external sharing pursuant to new or existing information sharing access agreement (MOU, MOA, LOI, etc.)?</b>	Existing Please describe applicable information sharing governance in place: For sharing information outside of DHS, (b) (7)(E) will follow CBP's process for sharing information (written request for authorization submitted to the CBP Privacy Office, followed by the submission of the DHS Form 191 to Privacy after the information has been released). In exigent circumstances

<sup>3</sup> 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.

<sup>4</sup> 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.





	<p><b>(b) (7)(E)</b> may pass the information prior to coordinating with CBP Privacy, but will follow up no later than the next business day. <b>(b) (7)(E)</b> may enter into Information Sharing Agreements or Memorandums of Understanding with Federal Partners. These agreements will follow OI Staffing requirements and will involve OI Policy, CBP's Office of Chief Counsel and CBP Privacy.</p>
<p><b>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?</b></p>	<p><input type="checkbox"/> No.</p> <p><input checked="" type="checkbox"/> Yes. If yes, please list: <b>(b) (7)(E)</b> may assist with access to social media information and provide specific training related to access, use, and protection of PII.</p>
<p><b>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?</b></p>	<p><input type="checkbox"/> No. What steps will be taken to develop and maintain the accounting:</p> <p><input type="checkbox"/> Yes. In what format is the accounting maintained:</p>
<p><b>9. Is there a FIPS 199 determination?<sup>4</sup></b></p>	<p><input checked="" type="checkbox"/> Unknown.</p> <p><input type="checkbox"/> No.</p> <p><input type="checkbox"/> Yes. Please indicate the determinations for each of the following:</p> <p>Confidentiality:  <input type="checkbox"/> Low <input type="checkbox"/> Moderate <input type="checkbox"/> High <input type="checkbox"/> Undefined</p> <p>Integrity:  <input type="checkbox"/> Low <input type="checkbox"/> Moderate <input type="checkbox"/> High <input type="checkbox"/> Undefined</p>


<sup>4</sup> 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: <input type="checkbox"/> Low <input type="checkbox"/> Moderate <input type="checkbox"/> High <input type="checkbox"/> Undefined
--	---

### PRIVACY THRESHOLD REVIEW

(TO BE COMPLETED BY COMPONENT PRIVACY OFFICE)

<b>Component Privacy Office Reviewer:</b>	(b) (6), (b) (7)(C)
<b>Date submitted to Component Privacy Office:</b>	May 29, 2018
<b>Date submitted to DHS Privacy Office:</b>	June 13, 2018
<b>Component Privacy Office Recommendation:</b>	
<i>Please include recommendation below, including what new privacy compliance documentation is needed.</i>	
(b) (5), (b) (7)(E) 	





--

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

<b>DHS Privacy Office Reviewer:</b>	(b) (6), (b) (7)(C)
<b>PCTS Workflow Number:</b>	(b) (7)(E)
<b>Date approved by DHS Privacy Office:</b>	July 2, 2018
<b>PTA Expiration Date</b>	September 2, 2018

**DESIGNATION**

<b>Privacy Sensitive System:</b>	Yes If "no" PTA adjudication is complete.
<b>Category of System:</b>	IT System If "other" is selected, please describe: <a href="#">Click here to enter text.</a>
<b>Determination:</b>	<input type="checkbox"/> PTA sufficient at this time. <input type="checkbox"/> Privacy compliance documentation determination in progress. <input type="checkbox"/> New information sharing arrangement is required. <input type="checkbox"/> DHS Policy for Computer-Readable Extracts Containing Sensitive PII applies. <input type="checkbox"/> Privacy Act Statement required. <input checked="" type="checkbox"/> Privacy Impact Assessment (PIA) required. <input checked="" type="checkbox"/> System of Records Notice (SORN) required. <input type="checkbox"/> Paperwork Reduction Act (PRA) Clearance may be required. Contact your component PRA Officer. <input type="checkbox"/> A Records Schedule may be required. Contact your component Records Officer.
<b>PIA:</b>	<b>New PIA is required.</b> If covered by existing PIA, please list:
<b>SORN:</b>	<b>SORN coverage To Be Determined during the development of the PIA</b> If covered by existing SORN, please list: DHS/CBP-024 Intelligence Records System (CIRS) System of Records, September 21, 2017, 82 FR 44198
<b>DHS Privacy Office Comments:</b>	



*Please describe rationale for privacy compliance determination above.*

CBP Privacy is submitting this PTA because CBP's (b) (7)(E) is a collaborative effort between CBP's Office of Intelligence (OI) and the Office of Professional Responsibility (OPR) to identify

(b) (7)(E)

(b) (7)(E) will require the collection of PII that will be limited to individuals (b) (7)(E) (b) (7)(E)

(b) (7)(E) will collect PII through social media posts made in public forums, reports from concerned citizens, media reporting, and (b) (7)(E)

(b) (7)(E)

(b) (7)(E) Information acquired will be evaluated by CBP personnel (b) (7)(E)

(b) (7)(E)

(b) (7)(E) No PII, including but not limited to screennames, social media handles, and IP address will be retained unless it is in support of the (b) (7)(E)

(b) (7)(E)

The DHS Privacy Office agrees that this initiative is privacy-sensitive, requiring PIA and SORN coverage. CBP Privacy is required to complete a New PIA to discuss the new information collection used to (b) (7)(E)

(b) (7)(E)

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

(b) (7)(E)

(b) (7)(E)

**The DHS Privacy Office requires that a training be created for all individuals supporting the search and analysis of social media for CBP employees who are trained as Law Enforcement Officers/Agents, who access, use, and protect PII to determine what is and is not a 1<sup>st</sup> Amendment protected activity.**



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)

(b) (7)(E) during the trial; and b) the limited timeframe of the potential collection (limited to the trial period only).

(b) (5)

**This PTA will expire on September 2<sup>nd</sup>, 2018 due to the reliance of a PIA and potentially a SORN.**





## 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<sup>1</sup>:

- 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

---

<sup>1</sup> 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](#).



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.





## 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: Customs and Border Protection**

**Contact Information:** (b) (6), (b) (7)(C) Director, (b) (7)(E) Office of Intelligence and Investigative Liaison (b) (6), (b) (7)(C)

**Counsel<sup>2</sup> Contact Information:** (b) (6), (b) (7)(C) Office of Chief Counsel, Enforcement Section

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

- **Automated Targeting System- Targeting Framework.**

Applicable Privacy Impact Assessment(s) (PIA):

DHS/CBP/PIA-006(b) [Automated Targeting System \(ATS\) Update](#), June 1, 2012. Per the ATS PIA, ATS maintains the official record “for certain law enforcement and/or intelligence data, reports, and projects developed by CBP analysts that may include public source information;”

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

[DHS/CBP-006 - Automated Targeting System](#) May 22, 2012, 77 FR 30297. Categories of records includes “Operational and analytical reports and/or projects developed that may include public source information and/or classified information obtained by users/analysts for reference or incorporation into the report or project.”

---

<sup>2</sup> Counsel listed here must certify that appropriate authority exists to engage in particular operational activities involving social media.



## DHS OPERATIONAL USE OF SOCIAL MEDIA

### SPECIFIC QUESTIONS

1. Describe the category of use for collecting personally identifiable information from social media sources. Examples include: law enforcement intelligence, criminal investigations, background investigations, administrative investigations, professional responsibility investigations, benefit or employment determinations, or situational awareness. If use does not fit into one of these categories, please describe in full below. If your component has multiple categories of use, please submit separate template for each category.

The personnel anticipated to use social media under this Border Encounter SMOUT include CBP Officers (CBPO) and Border Patrol Agents (BPA). This SMOUT encompasses (b) (7)(E) only, as defined in CBP Directive 5410-003, (b) (7)(E). After determining a traveler requires additional inspection, CBP Officers and Border Patrol Agents perform checks on biographic information provided by the traveler at or between Ports of Entry. CBP personnel who (b) (7)(E) [redacted] may access and review information, at their discretion, to perform queries on travelers' biographic information as they are undergoing secondary examination at a Port of Entry or between the ports of entry. Information gained through these operations may only be used by CBP personnel consistent with the legal authority of CBP, including admissibility determinations and other decisions as part of the inspection process. Information gained via social media as revealed by (b) (7)(E) [redacted] may be retained in records of examinations or case files in the Automated Targeting System's Targeting Framework (ATS-TF), if deemed necessary (b) (7)(E) [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]



CBP personnel may use mechanisms, such as the (b) (7)(E) (b) (7)(E) to access social media websites normally restricted from CBP workstations. (b) (7)(E)

(b) (7)(E) Information collected using social media is stored in the (b) (7)(E) (b) (7)(E)

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

Under section 235 of the Immigration and Nationality Act and its implementing regulations, CBP Officers and Border Patrol Agents have several enforcement authorities and responsibilities associated with inspections at a port of entry. 8 U.S.C. § 1225; *see also* 8 CFR 287.2 (stating that a special agent in charge, port director, or chief patrol agent shall initiate an investigation when he has reason to believe there has been a criminal immigration violation); 8 CFR 287.4 (stating that several positions within Border Patrol may issue subpoenas to be used in criminal or civil investigations); 8 CFR 287.9 (stating that Border Patrol agents must obtain a search warrant prior to conducting a search in a criminal investigation unless a specific exemption to the warrant requirement is authorized by statute or recognized by courts). *See also* 19 U.S.C. §§ 482, 1467, 1496, 1582, and 1589a, and 19 CFR Part 162.

(b) (5)

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

In development.       Operational. Date first launched:  
Unknown

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

Attached are the CBP Directive and Rules of Behavior.



5. Please describe the Rules of Behavior in effect for the listed operational use of social media. If users do NOT follow a particular Rule, please detail reasoning for not following that Rule:

a) *Equipment.* Use only government-issued equipment when engaging in the operational use of social media;

Yes.  No. If not, please explain:

b) *Email and accounts.* Use online screen names or identities that indicate an official DHS affiliation and use DHS email addresses to open accounts used when engaging in social media in the performance of their duties;

(b) (7)(E)

c) *Public interaction.* Access publicly available information through social media only by reviewing posted information without interacting with any individual who posted the information;

(b) (7)(E)

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

Yes.  No. If not, please explain:

(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:

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: December 17, 2015

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-006(b) Automated Targeting System (ATS) Update (June 1, 2012)

SORN: DHS/CBP-006 - Automated Targeting System May 22, 2012, 77 FR 30297

### 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.

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



- A SORN is required:
  - New.
  - Updated. <Please include the name and number of SORN to be updated here.>

### DHS PRIVACY OFFICE COMMENTS

The DHS Privacy office finds that CBP's use of social media for Border Encounter Research is consistent with existing privacy compliance documentation and the DHS MD 110-01 requirements.

CBP will conduct attributable, (b) (7)(E), (b) (5) only. CBP Officers and Border Patrol Agents (b) (7)(E)

CBP does not (b) (7)(E)  
(b) (7)(E)

Any information collected from social media will be stored within the CBP Automated Targeting System (ATS), Targeting Framework (TF) module. Per the 2012 ATS PIA, (b) (7)(E)

[Redacted text block]



## 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<sup>1</sup>:

- 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.

---

<sup>1</sup> 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:** Customs and Border Protection

**Contact Information:** (b) (6), (b) (7)(C) Director, (b) (6), (b) (7)(C) Office of Intelligence and Investigative Liaison (b) (6), (b) (7)(C)

**Counsel<sup>2</sup> Contact Information:** (b) (6), (b) (7)(C) Office of Chief Counsel, Enforcement Section

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

- **Automated Targeting System- Targeting Framework.**

Applicable Privacy Impact Assessment(s) (PIA):

DHS/CBP/PIA-006(b) [Automated Targeting System \(ATS\) Update](#), June 1, 2012. Per the ATS PIA, ATS maintains the official record “for certain law enforcement and/or intelligence data, reports, and projects developed by CBP analysts that may include public source information;”

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

[DHS/CBP-006 - Automated Targeting System](#) May 22, 2012, 77 FR 30297. Categories of records includes “Operational and analytical reports and/or projects developed that may include public source information and/or classified information obtained by users/analysts for reference or incorporation into the report or project.”

- **Analytical Framework for Intelligence**

DHS/CBP/PIA-010 – [Analytical Framework for Intelligence](#) (AFI), June 1, 2012. Per the AFI PIA § 2.1 Identify the information the project collects, uses, disseminates, or maintains: “... DHS AFI analysts may upload information that the user believes is relevant to a project, including information publicly available on the Internet.”

[DHS/CBP-017 – Analytical Framework for Intelligence System](#) June 7, 2012 77 FR 13813. Per the Record Source Categories: “Additionally, AFI permits analysts to upload and store any information from any source including public and commercial sources, which may be relevant to projects, responses to RFIs, or final intelligence products.”

---

<sup>2</sup> Counsel listed here must certify that appropriate authority exists to engage in particular operational activities involving social media.



## DHS OPERATIONAL USE OF SOCIAL MEDIA

### SPECIFIC QUESTIONS

1. Describe the category of use for collecting personally identifiable information from social media sources. Examples include: law enforcement intelligence, criminal investigations, background investigations, administrative investigations, professional responsibility investigations, benefit or employment determinations, or situational awareness. If use does not fit into one of these categories, please describe in full below. If your component has multiple categories of use, please submit separate template for each category.

The personnel anticipated to use social media under this SMOUT include CBP Intelligence Research Specialists, CBP Officers, Border Patrol Agents, and Air & Marine personnel. This SMOUT encompasses both (b) (7)(E)

(b) (7)(E) CBP personnel who receive specific prior supervisory approval may

(b) (7)(E)

(b) (7)(E) Under this SMOUT, CBP

personnel may use mechanisms, (b) (7)(E)

(b) (7)(E) (b) (7)(E)

Information gained through these operations may only be used consistent with the legal authorities of CBP. For example, this may include (b) (7)(E)

(b) (7)(E)

(b) (7)(E) Any

information gained via social media as (b) (7)(E)

may be retained, (b) (7)(E)

in the Automated Targeting System's Targeting Framework (ATS-TF) or the Analytical Framework for Intelligence. (b) (7)(E)

(b) (7)(E)

(b) (7)(E)

. This information may be stored in AFI or ATS-TF.

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

Under 235 of the Immigration and Nationality Act and its implementing regulations CBP Officers and Border Patrol Agents have several enforcement authorities and responsibilities associated with inspections at a port of entry. 8 U.S.C. § 1225; see also 8 CFR 287.2 (stating that a special agent in charge, port



director, or chief patrol agent shall initiate an investigation when he has reason to believe there has been a criminal immigration violation); 8 CFR 287.4 (stating that several positions within Border Patrol may issue subpoenas to be used in criminal or civil investigations); 8 CFR 287.9 (stating that Border Patrol agents must obtain a search warrant prior to conducting a search in a criminal investigation unless a specific exemption to the warrant requirement is authorized by statute or recognized by courts). *See also* 19 U.S.C. § 482, 1467, 1496, 1582, and 1589a, and 19 CFR Part 162.

(b) (5)



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

In development.  Operational. Date first launched: Unknown

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

Attached are the CBP Directive and Rules of Behavior.

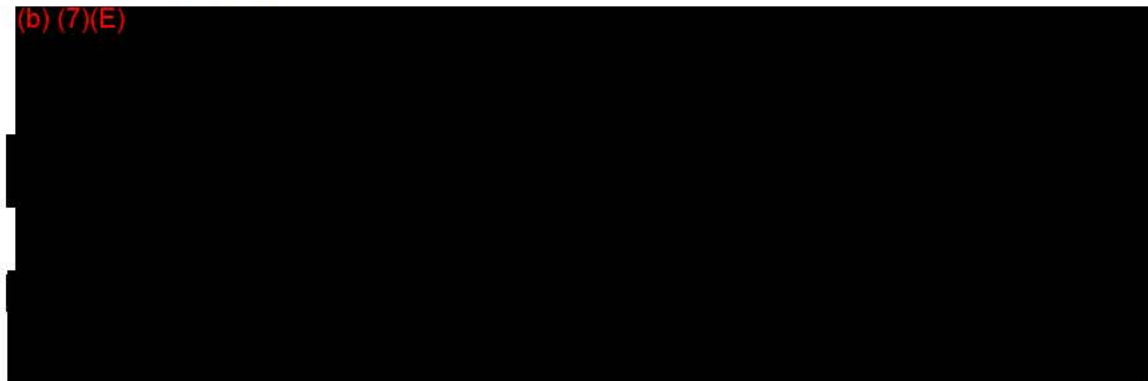
5. Please describe the Rules of Behavior in effect for the listed operational use of social media. If users do NOT follow a particular Rule, please detail reasoning for not following that Rule:

a) *Equipment.* Use only government-issued equipment when engaging in the operational use of social media;

Yes.  No. If not, please explain:

b) *Email and accounts.* Use online screen names or identities that indicate an official DHS affiliation and use DHS email addresses to open accounts used when engaging in social media in the performance of their duties;

(b) (7)(E)







- c) *Public interaction.* Access publicly available information through social media only by reviewing posted information without interacting with any individual who posted the information;

(b) (7)(E)



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

(b) (7)(E)



- e) *PII collection:* Collect the minimum PII necessary for the proper performance of their authorized duties except for systems subject to Final Rules for Exemption from certain aspects of the Privacy Act;

Yes.       No. If not, please explain:

- f) *PII safeguards.* Protect PII as required by the Privacy Act (if applicable) and DHS privacy policy;

Yes.       No. If not, please explain:

- g) *Documentation.* Document operational use of social media, including date, site(s) accessed, information collected and how it was used.

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:

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: May 13, 2015

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-006 ATS

SORN: DHS/CBP-006 ATS

### 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.

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

A SORN is required:

New.

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



## DHS PRIVACY OFFICE COMMENTS

CBP's use of social media for Operational Awareness is compliant with the DHS social media directive MD 110-01-011.

This SMOUT is intended to address (b) (7)(E). The ATS PIA referenced references CBP's use of information on the internet. The CBP Directive on the Operational Use of Social Media, CBP defines (b) (7)(E) as follows:

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

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

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



## 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:

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](#));

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.





## 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

**Name of SMOUT:** Border Patrol Intelligence – (b) (7)(E)

**Date submitted for review:** November 23, 2015

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

**Contact Information:** Assistant Chief (b) (6), (b) (7)(C) United States Border Patrol.  
(b) (6), (b) (7)(C)

**Counsel Contact Information:** (b) (6), (b) (7)(C) Office of Chief Counsel, Enforcement

**IT System(s) where social media data is stored:** Automated Targeting System-Targeting Framework and the Analytical Framework for Intelligence (if included in a finished intelligence product)

*Applicable Privacy Impact Assessment(s) (PIA):*

- DHS/CBP/PIA-006(e) [Automated Targeting System \(ATS\) Update](#), January 13, 2017. Per the ATS PIA, ATS maintains the official record “for certain law enforcement and/or intelligence data, reports, and projects developed by CBP analysts that may include public source information;”
- DHS/CBP/PIA-010a – [Analytical Framework for Intelligence](#) (AFI), September 1, 2016. Per the AFI PIA § 2.1 Identify the information the project collects, uses, disseminates, or maintains: “... DHS AFI analysts may upload information that the user believes is relevant to a project, including information publicly available on the Internet.”

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

**Raw intelligence collected by CBP is covered by:** DHS/CBP-024 Intelligence Records System (CIRS), September 21, 2017 82 FR 44198. This system of records allows CBP to collect and consolidate information from multiple sources, including law enforcement agencies and agencies of the U.S. Intelligence Community, in order to enhance CBP’s ability to: Identify, apprehend, or prosecute individuals who pose a potential law enforcement or security risk; aid in the enforcement of the customs and immigration laws, and other laws enforced by DHS at the border; and enhance U.S. border security.

Records maintained within the CIRS system of records include information collected by CBP for an intelligence purpose that is not covered by an existing DHS SORN and finished intelligence products. This information may include:



# Homeland Security

The Privacy Office  
U S Department of Homeland Security  
Washington, DC 20528  
202-343-1717, pia@dhs.gov  
www.dhs.gov/privacy

- Biographic information (name, date of birth, Social Security number, alien registration number, citizenship/immigration status, passport information, addresses, phone numbers, etc.);
- Records of immigration enforcement activities or law enforcement investigations/activities;
- Information (including documents and electronic data) collected by CBP from or about individuals during investigative activities and border searches;
- Records of immigration enforcement activities and law enforcement investigations/activities that have a possible nexus to CBP's law enforcement and immigration enforcement responsibilities or homeland security in general;
- Law enforcement, intelligence, crime, and incident reports (including financial reports under the Bank Secrecy Act and law enforcement bulletins) produced by DHS and other government agencies;
- U.S. visa, border, immigration, and naturalization benefit data, including arrival and departure data;
- Terrorist watchlist information and other terrorism-related information regarding threats, activities, and incidents;
- Lost and stolen passport data;
- Records pertaining to known or suspected terrorists, terrorist incidents, activities, groups, and threats;
- CBP-generated intelligence requirements, analysis, reporting, and briefings;
- Information from investigative and intelligence reports prepared by law enforcement agencies and agencies of the U.S. foreign intelligence community;
- **Articles, public-source data (including information from social media), and other published information on individuals and events of interest to CBP;**
- Audio and video records retained in support of CBP's law enforcement, national security, or other homeland security missions;
- Records and information from government data systems or retrieved from commercial data providers in the course of intelligence research, analysis, and reporting;
- Reports of suspicious activities, threats, or other incidents generated by CBP or third parties;
- Additional information about confidential sources or informants; and
- Metadata, which may include but is not limited to transaction date, time, location, and frequency.

**Finished Intelligence Products produced by CBP are covered by:** DHS/CBP-017 – Analytical Framework for Intelligence System, June 7, 2012 77 FR 13813. The purpose of this system is to enhance DHS's ability to: Identify, apprehend, and/or prosecute individuals who pose a potential law enforcement or security



# Homeland Security

The Privacy Office  
U S Department of Homeland Security  
Washington, DC 20528  
202-343-1717, pia@dhs.gov  
www.dhs.gov/privacy

risk; aid in the enforcement of the customs and immigration laws, and other laws enforced by DHS at the border; and enhance United States security. AFI uses data to:

- (1) Identify individuals, associations, or relationships that may pose a potential law enforcement or security risk, target cargo that may present a threat, and assist intelligence product users in the field in preventing the illegal entry of people and goods, or identifying other violations of law;
- (2) Allow analysts to conduct additional research on persons and/or cargo to understand whether there are patterns or trends that could identify potential law enforcement or security risks; and
- (3) Allow finished intelligence product users with a need to know to query or receive relevant finished intelligence products.



## 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 request access to social media for (b) (7)(E) as defined by the CBP Operational Use of Social Media Policy<sup>1</sup> for Border Patrol agents assigned to the Border Patrol Sector Intelligence Units (SIU), and the USBP Headquarters Intelligence Division (Border Patrol Intelligence Agents (BPA-Is), Supervisory Border Intelligence Agents (SBPA-Is) or Border Patrol Intelligence Enterprise (BPIE) intelligence analysts). The Sector Intelligence Unit (SIU) operates primarily at the tactical level, working in coordination with the HQ Intelligence Division, sector command staff and stations. The four primary functions of the SIU are to collect information that provides current intelligence, conduct targeted enforcement operations, provide analysis, and provide support to ongoing intelligence operations. This allows the SIU to produce sector level intelligence products for wider consumption, including federal, state, local, and tribal stakeholders.

The SIU will support sector command staff and respond to intelligence collection requirements both at the sector and national level. The SIU strives for integration with all stations within their respective sectors by working with station staff and collateral intelligence agents to address the station commander's objectives, gather information, and produce intelligence products for local and national consumption. In addition, SIU agents assigned to Border Patrol stations will act as subject matter experts to educate station personnel as to their role within the BPIE. The SIU has the following responsibilities:

- Understand intelligence priorities
- Produce quality, finished, information and intelligence products
- Ensure constant flow of information and intelligence
- Protect and promote intelligence integrity and objectivity
- Integrate intelligence into operational activities to reduce uncertainty
- Drive sector and station operations with collections and analytical support
- Understand and operate within intelligence doctrine, capabilities and limitations

<sup>1</sup> CBP Directive 5410-003 (January 2, 2015) defines

(b) (7)(E)

(b) (7)(E)





- Receive and incorporate feedback from agents, station staff and sector management

The primary mission of the SIU is to gather and synthesize information. To do so, Border Patrol agents who are assigned to the SIU or Headquarters Intelligence Division undergo specific training for the intelligence enterprise. All SIU personnel are trained and certified to perform the intelligence collection, management, and analytical functions necessary for their respective roles. Individuals responsible for providing that information must have the necessary skills and competencies necessary to provide that intelligence.

To accomplish their intelligence functions, these specialized USBP intelligence personnel must use (b) (7)(E)

(b) (7)(E)

### *General Procedures*

Consistent with the CBP Operational Use of Social Media Policy,<sup>2</sup> once this SMOUT has been approved by the DHS Privacy Office, there are additional procedural requirements for (b) (7)(E)

(b) (7)(E) Border Patrol agents who are assigned to Sector Intelligence Units or the USBP Headquarters Intelligence Division must obtain approval to use social media for (b) (7)(E) only when necessary for authorized law enforcement purposes with a clear nexus to their assigned duties and in conformance with existing (b) (7)(E)

(b) (7)(E)

### *Individual Access Requests*

Border Patrol agents who are assigned to (b) (7)(E) (b) (7)(E) (b) (5)

<sup>2</sup> CBP Directive 5410-003 (January 2, 2015) defines (b) (7)(E) (b) (7)(E)



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

(b) (5) [redacted]

Upon approval of this template and in accordance with the individual access procedures outlined in CBP Directive 5410-003, USBP intelligence personnel may use the (b) (7)(E) [redacted]

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

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

6 U.S.C. § 211(e) establishes the Border Patrol in CBP and sets forth certain statutory duties, including the responsibility to: “(A) serve as the law enforcement office of U.S. Customs and Border Protection with primary responsibility for interdicting persons attempting to illegally enter or exit the United States or goods being illegally imported into or exported from the United States at a place other than a designated port of entry; (B) deter and prevent the illegal entry of terrorists, terrorist weapons, persons, and contraband; and (C) carry out other duties and powers prescribed by the Commissioner.”

Under section 287(b) of the Immigration and Nationality Act (INA) (8 U.S.C. § 1357(b)), authorized Border Patrol agents “have the power and authority . . . to take and consider evidence concerning the privilege of any person to enter, reenter, pass through, or reside in the United States, or concerning any matter which is material or relevant to the enforcement of [the INA] . . .” See also 8 CFR 287.2 (stating that a special agent in charge, port director, or chief patrol agent shall initiate an investigation when he has reason to believe there has been a criminal immigration violation). Additionally, 19 U.S.C. § 1589a provides enforcement authority to customs officers, including Border Patrol agents.

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

(b) (5) [redacted]

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

In development.     Operational. Date first launched:

USBP use of social media for (b) (7)(E) [redacted] is pending the approval of this SMOUT.

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

Attached are the CBP Directive and Rules of Behavior.

**6. 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:**



*Equipment.* Use only government-issued equipment when engaging in the operational use of social media;

Yes.       No. If not, please explain:

*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)

*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)

(b) (7)(E)

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

(b) (7)(E)

(b) (7)(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:

*PII safeguards.* Protect PII as required by the Privacy Act (if applicable) and DHS privacy policy;

Yes.       No. If not, please explain:

*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:

*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.



# Homeland Security

The Privacy Office  
U S Department of Homeland Security  
Washington, DC 20528  
202-343-1717, pia@dhs.gov  
www.dhs.gov/privacy

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:

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: 11/27/2017

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-006 Automated Targeting System (ATS)

DHS/CBP/PIA-010 Analytical Framework for Intelligence (AFI)

**SORN:**

DHS/CBP-017 Analytical Framework for Intelligence System, June 7, 2012 77 FR 13813

DHS/CBP-024 Intelligence Records System (CIRS) System of Records, September 21, 2017, 82 FR 44198

1. (b) (7)(E) [Redacted list item]

(b) (5) [Redacted text block]

3. Rules of Behavior Content: (Check all items that apply.)



a. *Equipment.*

Users must use government-issued equipment. (b) (7)(E)  
(b) (7)(E)

Users must use government-issued equipment. (b) (7)(E)  
(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. (b) (7)(E)

(b) (7)(E)

e. *PII storage:*

PII is maintained in an exempted Privacy Act System of Records.

Please list applicable SORN here: DHS/CBP-017 Analytical Framework for Intelligence (AFI) System  
DHS/CBP-024 Intelligence Records System (CIRS)

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



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.
  - Updated. <Please include the name and number of PIA to be updated here.>
- A SORN is required:
  - 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 request for access to social media for (b) (7)(E), (b) (5) (b) (7)(E), (b) (5)s defined by the CBP Operational Use of Social Media Policy for U.S. Border Patrol (USBP) agents assigned to the Border Patrol Sector Intelligence Units (SIU), and the USBP Headquarters Intelligence Division. The primary mission of the SIU is to gather and synthesize information. (b) (7)(E), (b) (5)

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

Border Patrol agents who are assigned to SIU or the USBP Headquarters Intelligence Division (b) (7)(E) (b) (7)(E)  
 (b) (5)  
 (b) (7)(E)  
 (b) (7)(E)

. Any information collected from social media will be stored within the Automated Targeting System-Targeting Framework (ATS-TF) and the Analytical Framework for Intelligence (AFI) (if included in a finished intelligence product). Per the ATS PIA, ATS-TF allows authorized users to attach public source information, such as responsive Internet links and related documents, to an assigned report and/or project and search for any text contained within the system via full text search functionality. Per the AFI PIA, analysts may upload information that the user believes is relevant to a project, including information publicly available on the Internet.

SORN coverage for raw intelligence collected by CBP is covered by DHS/CBP-024 Intelligence Records System (CIRS), which covers the collection and consolidation of information from multiple sources, including law enforcement agencies and agencies of the U.S. Intelligence Community, in order to enhance CBP's ability to: identify, apprehend, or prosecute individuals who pose a potential law enforcement or





# Homeland Security

The Privacy Office  
U S Department of Homeland Security  
Washington, DC 20528  
202-343-1717, pia@dhs.gov  
www.dhs.gov/privacy

security risk; aid in the enforcement of the customs and immigration laws, and other laws enforced by DHS at the border; and enhance U.S. border security. Records maintained within the CIRS may include “articles, public-source data (including information from social media), and other published information on individuals and events of interest to CBP.” SORN coverage for finished intelligence products produced by CBP is provided by DHS/CBP-017 Analytical Framework for Intelligence System, which covers the collection of information to enhance DHS’s ability to: identify, apprehend, and/or prosecute individuals who pose a potential law enforcement or security risk; aid in the enforcement of the customs and immigration laws, and other laws enforced by DHS at the border; and enhance U.S. security.

# **U.S. Customs and Border Protection Operational Use of Social Media Rules of Behavior**

The following rules of behavior apply to all U.S. Customs and Border Protection (CBP) employees, contractors, and persons using CBP systems in furtherance of the CBP mission with access to social media sites and the public internet for the purposes of overseeing or conducting operational activities related to the mission of CBP. These activities may include, but are not limited to: determining admissibility, identity resolution, reconciling screening and targeting matches, counter-terrorism investigations, counter-narcotics investigations, smuggling investigations, trade and credential fraud investigations, interdictions, border and event security, enhancing general, operational awareness, and assisting in making benefit, personnel, or suitability determinations. These rules of behavior are separate and apart from those rules of behavior which cover accessing social media sites and the public internet for the purpose of communications and outreach with the public.

## **1. Social Media Access, Generally:**

- a. I understand that all activities of accessing restricted internet sites or access to social media sites will be in accordance with applicable law and DHS and CBP guidance.
- b. I understand that my access to social media under these specific rules of behavior does not include conducting communications and outreach with the public, and in connection with the Office of Public Affairs as directed in CBP Directive 5410-001B, Office of Public Affairs Roles, Functions and Responsibilities.
- c. I will only access those sites for which I require access to perform mission-related tasks as part of my official duties and for purposes that are authorized by statute, executive order, regulation, or policy. I will not attempt to access sites or perform actions that I am not authorized to access or perform.
- d. I understand that I must complete all required privacy training prior to receiving access to social media sites and that I will complete annual refresher training as long as access is still needed and approved by a Template.
- e. I understand that my access requirements will be reviewed on an annual basis and that my access can be terminated at any time if it is no longer needed due to a change in official duties, if I am no longer authorized to conduct activities requiring the access, if I am serving a suspension due to misconduct, if I am under a suspension of law enforcement authority, if I separate from CBP, or if I misuse my access.

**2. Overt Operational Use of Social Media and the Public Internet (Overt Research, Monitoring, and Engagement):**

- a. I will use only government-issued equipment, internet connections authorized to access social media through the DHS/CBP network (i.e., no “stand-alone” connections), government-approved accounts and government-approved email addresses when engaging in the overt operational use of social media and the public internet on behalf of CBP.
- b. I will only use screen names or identities that indicate an official DHS or CBP affiliation.
- c. I will not engage in the use of social media on government equipment or use any account created on behalf of CBP, for unofficial purposes.
- d. I will not use vulgar or abusive language, engage in personal attacks of any kind, or use offensive terms targeting individuals or groups while using social media or the public internet on behalf of DHS.
- e. I will not knowingly endorse commercial products, services or entities, nor will I knowingly endorse political parties, candidates or groups while using social media or the public internet on behalf of DHS.<sup>1</sup>
- f. I will not lobby members of Congress using DHS or any other appropriated resource via social media or the public internet.
- g. I will not use government resources to foster commercial interests or for individual profit.
- h. I will log off of or otherwise restrict access to any social media session when I am not personally attending to it.

**3. Data Protection for Overt Use:**

- a. I will not access information that is not publicly available, without consent.
- b. I will not interact with individuals who post the information, unless there is a specific and clearly articulated operational necessity to interact with individuals who post the information as defined in my authorized mission responsibilities.

---

<sup>1</sup> ‘Knowingly’ is included here because there is the possibility on social media sites like Facebook that one may be trying to click on another item and unknowingly click on a commercial product or political candidate, thereby endorsing the product or the political candidate. (b) (7)(E)

- c. I will only use the minimum amount of personally identifiable information (PII) necessary for the defined operational use of social media or the public internet.
- d. I will protect any PII in accordance with the Privacy Act (where applicable) and DHS and CBP privacy policy (e.g., PII obtained from a SORN and disclosed for a use in research, monitoring, or engagement will be accounted for on a DHS-191).
- e. I will not search social media sites or the public internet for or by PII unless this search is necessary for the purpose defined by my authorized operational use of social media.
- f. I will not access or post classified or otherwise protected information (e.g. For Official Use Only (FOUO)) using social media or the public internet (e.g., [REDACTED]).
- g. I will document my operational use of social media, including date, site(s) accessed, information collected, information disclosed for purposes of access, and how it was used in the same manner that CBP would document information collected during each of its operational activities.

**4. Undercover Operational Use of Social Media and the Public Internet (Masked Monitoring and Undercover Engagement):**

- a. I will use government-issued equipment, internet connections authorized to access social media through the DHS/CBP network (i.e., no “stand-alone” connections), government-approved accounts and government-approved email addresses, unless authorized by the terms of my assigned mission responsibilities, when engaging in the undercover operational use of social media and the public internet on behalf of CBP.
- b. I will not engage in use of social media on government equipment or use any account created on behalf of CBP for unofficial purposes.
- c. I will refrain from using vulgar or abusive language, engaging in personal attacks of any kind, or using offensive terms targeting individuals or groups while using social media or the public internet, unless it is necessary as defined by the scope of my masked or assumed identity in the context of my authorized mission responsibilities.
- d. I will not knowingly endorse commercial products, services or entities, nor will I knowingly endorse political parties, candidates or groups while using social



media or the public internet on behalf of DHS, unless authorized by the terms of the SMOUT for my undercover engagement.<sup>2</sup>

- e. I will not lobby members of Congress using DHS or any other appropriated resource via social media or the public internet, unless authorized by the terms of the SMOUT for my undercover engagement.
- f. I will not use government resources to foster commercial interests or for the appearance of individual profit, unless authorized by the terms of the SMOUT for my undercover engagement.
- g. I will log off of or otherwise restrict access to any social media session when I am not personally attending to it.

#### 5. Data Protection for Undercover Use:

- a. I will not access information that is not publicly available, without consent, unless authorized in the execution of the terms of my assigned mission responsibilities.
- b. I will not interact with individuals who post the information, unless there is a specific and clearly articulated operational necessity to interact with individuals who post the information as defined in my authorized mission responsibilities.
- c. I will only use the minimum amount of personally identifiable information (PII) necessary for the defined operational use of social media or the public internet.
- d. I will protect any PII in accordance with the Privacy Act (where applicable) and DHS and CBP privacy policy (e.g., PII obtained from a SORN and disclosed for a use in monitoring or engagement will be accounted for on a DHS-191).
- e. I will not search social media sites or the public internet for or using PII unless this search is necessary for the purpose defined by my authorized operational use of social media.
- f. I will not access or post classified or otherwise protected information (e.g., FOUO) using social media or the public internet (e.g., (b) (7)(E)).
- g. I will document my operational use of social media, including date, site(s) accessed, information collected, and how it was used in the same manner that

---

<sup>2</sup> 'Knowingly' is included here because there is the possibility on social media sites like Facebook that one may be trying to click on another item and unknowingly click on a commercial product or political candidate, thereby endorsing the product or the political candidate. (b) (7)(E)

CBP would document information collected during each of its operational activities.

**6. Incident Reporting:**

- I will promptly report suspected or confirmed IT security incidents (e.g., (b) (7)(E) \_\_\_\_\_), and per the DHS Handbook for Safeguarding Sensitive PII and the Privacy Incident Handling Guide (PIHG), report any privacy incidents (e.g., loss or compromise of sensitive PII) to the DHS IT Help Desk at (b) (7)(E) (b) (7)(E) and my supervisor.

**7. Accountability:**

- a. I understand that I have no expectation of privacy while using government Information Technology (IT) systems or any accounts created on behalf of CBP or in furtherance of CBP's mission.
- b. I understand that I will be held accountable for my actions while accessing and using government IT systems and social media sites and may face disciplinary action and/or criminal or civil prosecution for misuse. Additionally, misuse may lead to removal from position and/or termination.

**Acknowledgment Statement**

I acknowledge that I have read the rules of behavior; I understand them, and I will comply with them. I understand that failure to comply with these rules could result in verbal or written warning, removal of access to social media on behalf of CBP, reassignment to other duties, criminal or civil prosecution, or termination.

\_\_\_\_\_  
**Employee Signature**

\_\_\_\_\_  
**Date**

*Participating in the CBP Operational Use of Social Media Training is required and serves as acknowledgement and acceptance of these Rules of Behavior.*

**Date Training Completed:** \_\_\_\_\_

**Upon completing the signature, date, and training completion date portion, submit this to the Privacy and Diversity Office at (b) (7)(E) \_\_\_\_\_**