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

DHS OPERATIONAL USE OF SOCIAL MEDIA

This template is used to assess the Department's Operational Use of Social Media, consistent with Management Directive 110-01.

The DHS Privacy Office has created this template to determine privacy compliance with Management Directive 110-01, Privacy Policy for Operational Use of Social Media. For the purposes of the Management Directive and this template, "Operational Use" means authorized use of social media to collect personally identifiable information for the purpose of enhancing situational awareness, investigating an individual in a criminal, civil, or administrative context, making a benefit determination about a person, making a personnel determination about a Department employee, making a suitability determination about a prospective Department employee, or for any other official Department purpose that has the potential to affect the rights, privileges, or benefits of an individual. Operational use does not include the use of search engines for general Internet research, nor does it include the use of social media for professional development such as training and continuing education or for facilitating internal meetings. The following uses of social media are exempt from the Management Directive and are not subject to this requirement:

> 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.

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

DHS OPERATIONAL USE OF SOCIAL MEDIA

Please complete this form and send it to your Component Privacy Officer. Upon receipt, your Component Privacy Officer and the DHS Privacy Office will review this form and may request additional information.

Summary Information

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) @cCBP.DHS.GOV, (b) (6), (b) (7)(C)
Counsel Contact Information:	Marc Bennett Courey, 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:

- 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

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.

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

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[1] 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

[1] 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,[2] 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)

[2] CBP Directive 5410-003 (January 2, 2015) defines (b) (7)(E)

(b) (7)(E)

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

(b) (7)(E)

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)

(b) (7)(E)

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)

(b) (5)

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) 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:**

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

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)

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.

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:

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

DHS SOCIAL MEDIA DOCUMENTATION

(To be completed by the DHS Privacy Office)

DATE reviewed by the DHS Privacy Office: 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)

(b) (5)

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:

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

☐ 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) as 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)

Border Patrol agents who are assigned to SIU or the USBP Headquarters Intelligence Division (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

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.