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

PRIVACY THRESHOLD ANALYSIS (PTA)

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

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

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

Senior Director, Privacy Compliance
The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
Tel: 202-343-1717

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, on DHS Connect and directly from the DHS Privacy Office via email: pia@hq.dhs.gov, phone: 202-343-1717.

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

PRIVACY THRESHOLD ANALYSIS (PTA)

SUMMARY INFORMATION

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

PROJECT OR PROGRAM MANAGER

Name:	(b) (6), (b) (7)(C)		
Office:	**Office of Intelligence**	**Title:**	Program Manager
Phone:	(b) (6), (b) (7)(C)	**Email:**	(b) (6), (b) (7)(C) @cbp.dhs.gov

INFORMATION SYSTEM SECURITY OFFICER (ISSO) (IF APPLICABLE)

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

Specific PTA Questions

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

This PTA provides and 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) hrough 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) will collect PII through social media posts made in public forums, reports from concerned citizens, media reporting, and may receive (b) (7)(E) . Information acquired will be evaluated by CBP personnel (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 1st 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) [redacted] ersonnel will respect privacy settings on all platforms, and will only access publicly available information.

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

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

4. What specific information about individuals is collected, generated or retained?	
a. b.	(b) (7)(E) [redacted]

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

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

(b) (7)(E)

c.

d.

e.

4(a) Does the project, program, or system retrieve information by personal identifier?	☐ No. Please continue to next question. ☒ Yes. If yes, please list all personal identifiers used: include but not limited to: (b) (7)(E)

	(b) (7)(E) [redacted]
4(b) Does the project, program, or system use Social Security Numbers (SSN)?	☐ No. ☒ Yes. Entered as a case file within (b) (7)(E) [redacted] r received as part of existing partner agency case file
4(c) If yes, please provide the specific legal basis and purpose for the collection of SSNs:	Collection will be used for identity verification as part of a CBP [redacted] (b) (7)(E) [redacted] 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..
4(d) If yes, please describe the uses of the SSNs within the project, program, or system:	Identity verification.
4(e) If this project, program, or system is an information technology/system, does it relate solely to infrastructure?	☒ No. Please continue to next question. ☐ Yes. If a log kept of communication traffic, please answer the following question.

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

5. Does this project, program, or system connect, receive, or share PII with any other DHS programs or systems[4]?	☐ No. ☒ Yes. If yes, please list: (b) (7)(E) (b) (7)(E)
6. Does this project, program, or system connect, receive, or share PII with any external (non-DHS) partners or systems?	☐ No. ☒ 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.
6(a) Is this external sharing pursuant to new or existing information sharing access agreement (MOU, MOA, LOI, etc.)?	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

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

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

	(b) (7)(E) may pass the information prior to coordinating with CBP Privacy, but will follow up no later than the next business day. (b) (7)(E) 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.
7. Does the project, program, or system provide role-based training for personnel who have access in addition to annual privacy training required of all DHS personnel?	☐ No. ☒ Yes. If yes, please list: (b) (7)(E) may assist with access to social media information and provide specific training related to access, use, and protection of PII.
8. Per NIST SP 800-53 Rev. 4, Appendix J, does the project, program, or system maintain an accounting of disclosures of PII to individuals who have requested access to their PII?	☐ No. What steps will be taken to develop and maintain the accounting: ☐ Yes. In what format is the accounting maintained:
9. Is there a FIPS 199 determination?[4]	☒ Unknown. ☐ No. ☐ Yes. Please indicate the determinations for each of the following: Confidentiality: ☐ Low ☐ Moderate ☐ High ☐ Undefined Integrity: ☐ Low ☐ Moderate ☐ High ☐ Undefined

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

	Availability: ☐ Low ☐ Moderate ☐ High ☐ Undefined

PRIVACY THRESHOLD REVIEW

(TO BE COMPLETED BY COMPONENT PRIVACY OFFICE)

Component Privacy Office Reviewer:	(b) (6), (b) (7)(C)
Date submitted to Component Privacy Office:	**May 29, 2018**
Date submitted to DHS Privacy Office:	June 13, 2018

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

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

[redacted]

(TO BE COMPLETED BY THE DHS PRIVACY OFFICE)

DHS Privacy Office Reviewer:	(b) (6), (b) (7)(C)
PCTS Workflow Number:	**1164632**
Date approved by DHS Privacy Office:	July 2, 2018
PTA Expiration Date	September 2, 2018

DESIGNATION

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

Please describe rationale for privacy compliance determination above.

CBP Privacy is submitting this PTA because CBP' (b) (7)(E) s 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) will collect PII through social media posts made in public forums, reports from concerned citizens, media reporting, and (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 the (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)

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 1st 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 2nd, 2018 due to the reliance of a PIA and potentially a SORN.