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

PRIVACY THRESHOLD ANALYSIS (PTA)

SUMMARY INFORMATION

Project or Program Name:	**ESTA Social Media Tool 2 Pilot Evaluation**		
Component:	Customs and Border Protection (CBP)	**Office or Program:**	OFO (b) (7)(E)
Xacta FISMA Name (if applicable):	(b) (7)(E)	**Xacta FISMA Number (if applicable):**	(b) (7)(E)
Type of Project or Program:	**Pilot**	**Project or program status:**	**Pilot**
Date first developed:	**January 1, 2017**	**Pilot launch date:**	**January 8, 2018**
Date of last PTA update	**N/A**	**Pilot end date:**	**December 31, 2018**
ATO Status (if applicable)	**Complete**	**ATO expiration date (if applicable):**	**January 25, 2020**

PROJECT OR PROGRAM MANAGER

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

INFORMATION SYSTEM SECURITY OFFICER (ISSO) (IF APPLICABLE)

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

SPECIFIC PTA QUESTIONS

1. Reason for submitting the PTA: New PTA

CBP is submitting this PTA to test a secondary Electronic System Travel Authorization (ESTA) social media vetting tool, (b) (7)(E) CBP previously conducted the ESTA Social Media Tool Pilot Evaluation (June 11, 2016-September 9, 2016) in which CBP supported DHS S&T's lead testing the efficacy of an initial commercial capability in this space. The PTA for that effort was adjudicated August 15, 2016.

(b) (7)(E)

During this pilot, which will occur from January 8, 2018 to December 31, 2018, CBP will evaluate ESTA cases in the following scenarios:

1. ESTA Cases Referred for Manual Review (including those being considered for a waiver)
   a. In these cases, CBP officers working on ESTA vetting have requested social media review internally within CBP (b) (7)(E) (b) (7)(E) to help determine eligibility and admissibility under the Visa Waiver Program.
   b. The operational pilot will assist with the review of these cases using this new tool to support adjudicatory decisions by (b) (7)(E) responsible for adjudication of the applications in question who will manually review the results.
2. Other ESTA Cases that may require additional review by the ESTA team (e.g. cases of concern for (b) (7)(E)
   a. (b) (7)(E)
   b. (b) (7)(E)

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

In all cases, CBP will access publicly available information in accordance with its authorities. This means that all searches will be conducted using open source material and that CBP Officers must respect individuals' privacy settings and access only information that is publicly available.

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?

(b) (7)(E) [redacted]. As part of this pilot, CBP will also collect publicly available information from social media platforms to assist in assessing the eligibility of ESTA applicants to travel under Visa Waiver Program (VWP). Any derogatory information collected from social media and deemed operationally relevant will be stored in ATS-TF.

[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.

The full list of ESTA application fields is below:
- Full name (first, middle, and last);
- Other names or aliases, if available;
- Date of birth;
- City and country of birth;
- Gender;
- Email address;
- Telephone number (home, mobile, work, other);
- Home address (address, apartment number, city, state/region);
- Internet protocol (IP) address;
- ESTA application number;
- Country of residence;
- Social media handles

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

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

5. Does this project, program, or system connect, receive, or share PII with any other DHS programs or systems[4]?	☐ No. ☒ Yes. If yes, please list: Any PII or potentially derogatory information identified and retained will be stored within ATS-TF.
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: Information regarding ESTA applications will be loaded into (b) (7)(E) (b) (7)(E)
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: (b) (7)(E) (b) (7)(E)
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: All CBP Officers, Agents, Analysts, and Contractors using Social Media for operational purposes must complete the CBP Social Media Training and Rules of Behavior. (b) (7)(E)

8. Per NIST SP 800-53 Rev. 4, Appendix J, does the project, program, or system maintain an accounting of disclosures of PII to individuals/agencies who have requested access to their PII?	☒ No. What steps will be taken to develop and maintain the accounting: (b) (7)(E) ☐ 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 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:	**December 6, 2017**

[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.

Date submitted to DHS Privacy Office:	December 20, 2017

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:	**1155460**
Date approved by DHS Privacy Office:	January 5, 2018
PTA Expiration Date	January 5, 2021

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:	**System covered by existing PIA** If covered by existing PIA, please list: DHS/CBP/PIA-006(b) Automated Targeting System (ATS) DHS/CBP/PIA-007(g) Electronic System for Travel Authorization (ESTA)
SORN:	System covered by existing SORN If covered by existing SORN, please list: DHS/CBP-006 Automated Targeting System, May 22, 2012, 77 FR 30297 DHS/CBP-009 Electronic System for Travel Authorization, September 2, 2016, 81 FR 60713

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

CBP is submitting this PTA to discuss the next update for the ESTA Social Media Pilot. This update involves use of a new social media vetting tool, (b) (7)(E)

(b) (7)(E)

The DHS Privacy Office finds this initiative privacy-sensitive.

Coverage is provided by DHS/CBP/PIA-007 ESTA and the DHS/CBP-009 ESTA. The Privacy Office agrees that coverage for this pilot is also provided under DHS/CBP/PIA-006 ATS, which outlines CBP's use of decision support tools in order to compare traveler information against law enforcement, intelligence, and other enforcement data. Additionally, this PIA outlines the querying of publicly available information in support of the vetting process. The DHS Privacy Office also agrees that SORN coverage is provided by the DHS/CBP-006 ATS SORN, which notes that CBP collects information on

individuals whom may be subject to closer questioning or examination upon arrival to or departure from the United States or who may require further examination, as well as those who may pose a risk to border security or public safety, may be a terrorist or suspected terrorist, or may otherwise be engaged in activity in violation of U.S. law.

In all cases, CBP will access publicly available information in accordance with its authorities. This means that all searches will be conducted using open source material and that CBP Officers must respect individuals' privacy settings and access only information that is publicly available.