



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:	(b) (7)(E) - Pilot Evaluation		
Component:	Customs and Border Protection (CBP)	Office or Program:	OFO (b) (7)(E)
Xacta FISMA Name (if applicable):	Click here to enter text.	Xacta FISMA Number (if applicable):	Click here to enter text.
Type of Project or Program:	Pilot	Project or program status:	Pilot
Date first developed:	November 5, 2016	Pilot launch date:	March 13, 2017
Date of last PTA update	N/A	Pilot end date:	December 31, 2017
ATO Status (if applicable)	Choose an item.	ATO expiration date (if applicable):	Click here to enter a date.

PROJECT OR PROGRAM MANAGER

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

INFORMATION SYSTEM SECURITY OFFICER (ISSO) (IF APPLICABLE)

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



SPECIFIC PTA QUESTIONS

1. Reason for submitting the PTA: New PTA	
<p>U.S. Customs and Border Protection (CBP) is responsible for securing the borders of the United States while facilitating legitimate travel and trade to and from the same. CBP is entering into a testing and evaluation pilot with <i>MITRE</i> to test and evaluate their (b) (7)(E). This pilot will assess the (b) (5), (b) (7)(E).</p> <p>(b) (7)(E) already in use by CBP (and across DHS).</p> <p>CBP currently uses publicly available social media information – consistent with previously approved Social Media Operational Use Templates (SMOUTs) – to conduct social media analysis in support of its border security mission. In particular, one of CBP’s approved SMOUTs permits CBP to use (b) (7)(E) (b) (7)(E) to conduct thorough social media research in accordance with the terms of use of various social media platforms and providers. In all cases involved in this pilot, CBP will only access publicly available information in accordance with the privacy policies of the underlying social media or open source platforms analyzed. This means that all searches will be conducted (b) (7)(E).</p> <p>(b) (7)(E)</p> <p>Analysis during this testing and evaluation pilot will be focused primarily on (b) (7)(E). However, research using publicly available information may be conducted (b) (7)(E) pursuant to CBP’s law enforcement authorities as deemed necessary to support CBP operations. As a pilot, this study will be fluid and allow for a range of information to be researched related to CBP’s mission.</p> <p>(b) (7)(E)</p>	

2. Does this system employ any of the following technologies:	<input type="checkbox"/> Closed Circuit Television (CCTV) <input checked="" type="checkbox"/> Social Media
--	---

(b) (7)(E) is also used by S&T for its various social media pilots, including the ESTA Social Media Vetting Pilot.

(b) (7)(E)



<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>	<input checked="" type="checkbox"/> Web portal ³ (e.g., SharePoint) <input type="checkbox"/> Contact Lists <input type="checkbox"/> None of these
--	--

<p>3. From whom does the Project or Program collect, maintain, use, or disseminate information? <i>Please check all that apply.</i></p>	<input type="checkbox"/> This program does not collect any personally identifiable information ⁴ <input checked="" type="checkbox"/> Members of the public <input checked="" type="checkbox"/> DHS employees/contractors (list components): <input checked="" type="checkbox"/> Contractors working on behalf of DHS <input type="checkbox"/> Employees of other federal agencies
--	--

4. What specific information about individuals is collected, generated or retained?	
<p>Information collected from DHS employees/contractors (CBP only) and contractors working on behalf of DHS will consist of email addresses (their work email address and/or a Gmail address) and log-in information to the (b) (7)(E)</p> <p>Publicly available information regarding subjects of interest to this pilot study may include (b) (7)(E)</p> <p>Such information may be collected during the course of the pilot in support of the CBP border security mission. Any derogatory information collected from social media and deemed operationally necessary will be stored in the ATS Targeting Framework (ATS-TF) pursuant to existing data retention policy and the approved SMOUT.</p> <p>Further examples of elements of publicly available PII that may be collected during this pilot, if available, include:</p>	

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)

Data collected from publicly available social media is covered under ATS:

1. 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;”
2. 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.”

4(a) Does the project, program, or system retrieve information by personal identifier?	<input checked="" type="checkbox"/> No. Please continue to next question. <input type="checkbox"/> Yes. If yes, please list all personal identifiers used:
4(b) Does the project, program, or system use Social Security Numbers (SSN)?	<input checked="" type="checkbox"/> No. <input type="checkbox"/> 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? <i>For example, is the system a Local Area Network (LAN) or Wide Area Network (WAN)?</i>	<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.



4(f) If header or payload data⁵ 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 systems⁴?	<input type="checkbox"/> No. <input checked="" type="checkbox"/> Yes. If yes, please list: Any identified PII or potentially derogatory information 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?	<input checked="" type="checkbox"/> No. <input type="checkbox"/> Yes. If yes, please list:
6(a) Is this external sharing pursuant to new or existing information sharing access agreement (MOU, MOA, LOI, etc.)?	N/A
7. Does the project, program, or system provide role-based training for personnel who have access in addition to annual privacy training required of all DHS personnel?	<input type="checkbox"/> No. <input checked="" type="checkbox"/> Yes. If yes, please list: MITRE has available documentation on the use of the (b) (7)(E) (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?	<input type="checkbox"/> <input checked="" type="checkbox"/> Yes. In what format is the accounting maintained: DHS 191 Form which will be provided to the CBP Privacy and Diversity Office should any information from ATS-TF be disclosed.

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.



<p>9. Is there a FIPS 199 determination?⁶</p>	<p><input type="checkbox"/> Unknown.</p> <p><input type="checkbox"/> No.</p> <p><input checked="" type="checkbox"/> Yes. Please indicate the determinations for each of the following:</p> <p>Confidentiality: <input type="checkbox"/> Low <input checked="" type="checkbox"/> Moderate <input type="checkbox"/> High <input type="checkbox"/> Undefined</p> <p>Integrity: <input checked="" type="checkbox"/> Low <input type="checkbox"/> Moderate <input type="checkbox"/> High <input type="checkbox"/> Undefined</p> <p>Availability: <input checked="" type="checkbox"/> Low <input type="checkbox"/> Moderate <input type="checkbox"/> High <input type="checkbox"/> Undefined</p>
---	---

PRIVACY THRESHOLD REVIEW

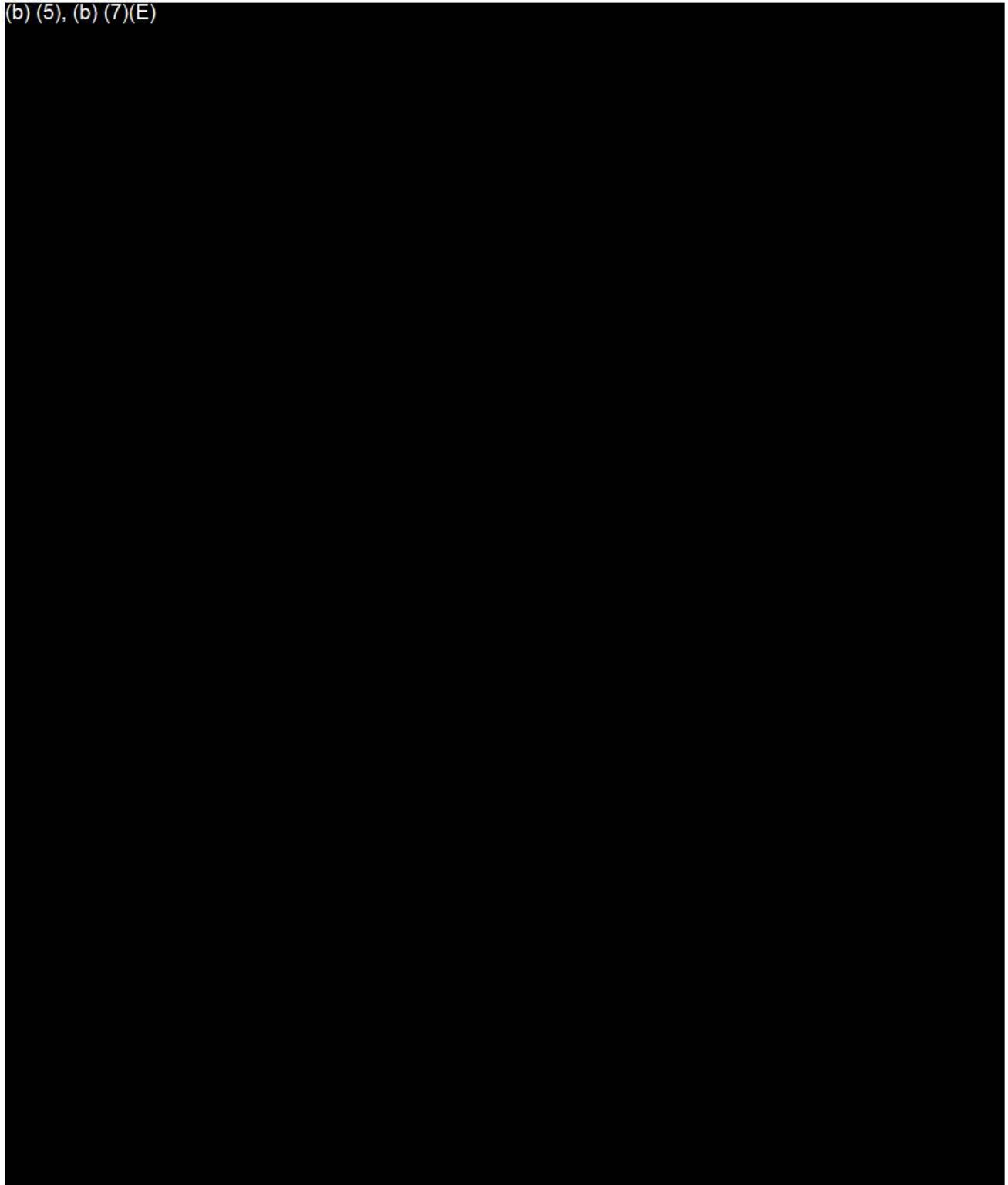
(TO BE COMPLETED BY COMPONENT PRIVACY OFFICE)

Component Privacy Office Reviewer:	(b) (6), (b) (7)(C)
Date submitted to Component Privacy Office:	March 13, 2017
Date submitted to DHS Privacy Office:	March 14, 2017
Component Privacy Office Recommendation:	
<i>Please include recommendation below, including what new privacy compliance documentation is needed.</i>	
(b) (7)(E), (b) (5)	
(b) (7)(E), (b) (5)	

⁶ FIPS 199 is the [Federal Information Processing Standard](#) Publication 199, Standards for Security Categorization of Federal Information and Information Systems and is used to establish security categories of information systems.



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





(TO BE COMPLETED BY THE DHS PRIVACY OFFICE)

DHS Privacy Office Reviewer:	(b) (6), (b) (7)(C)
PCTS Workflow Number:	1140140
Date approved by DHS Privacy Office:	March 16, 2017
PTA Expiration Date	March 16, 2020

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:	<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.
PIA:	System covered by existing PIA If covered by existing PIA, please list: DHS/CBP/PIA-006 Automated Targeting System (ATS) (b) (5)
SORN:	System covered by existing SORN



If covered by existing SORN, please list: DHS/ALL-004 General Information Technology Access Account Records System (GITAARS), November 27, 2012, 77 FR 70792
DHS/CBP-006 Automated Targeting System, May 22, 2012, 77 FR 30297

DHS Privacy Office Comments:

Please describe rationale for privacy compliance determination above.

CBP is submitting this PTA to discuss its use of the (b) (7)(E) in a testing and evaluation pilot. (b) (7)(E)

(b) (7)(E)

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

CBP currently uses publicly available social media information to conduct analysis in support of its border security mission. In particular, one of CBP's approved SMOUTs permits CBP to use (b) (7)(E) (b) (7)(E) to conduct thorough social media research in accordance with the terms of use of various social media platforms and providers. In all cases involved in this pilot, CBP will only access publicly available information in accordance with the privacy policies of the underlying social media or open source platforms analyzed.

CBP may collect PII from publicly available information regarding subjects of interest to this pilot in support of the CBP border security mission. Any derogatory information collected from social media and deemed operationally necessary will be stored in the ATS Targeting Framework (ATS-TF) pursuant to existing data retention policy and the approved SMOUT. The collection of this information is covered by the DHS/CBP/PIA-006 Automated Targeting System and the DHS/CBP-006 Automated Targeting System SORN.

Additionally, in order to access the (b) (7)(E) DHS collects email addresses and log-in information from DHS employees/contractors. This collection of information is covered by the DHS/ALL-004 GITAARS SORN.

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

This PTA expires in 3 years.