

INFORMATION ISSUE PAPER

Office of Field Operations
National Targeting Center (NTC)
October 6, 2016

Action Required: Information Only

Time Constraint: None

Issue: Privacy and CRCL groups have opposed CBP's efforts, with the Department, to modify the ESTA application to include the voluntary provision of social media handles. CBP has gone through a 60-day public comment period on its FRN proposing this voluntary provision, met with OMB to discuss and defend this request, added an additional 30-day comment period, and responded in full to all public inquiries about this addition. This final 30-day comment period is over and CBP will meet, with Department representation, with OMB on 6 October 2016 to advocate for the approval of the ESTA social media modification.

Executive Summary: Despite incorporating social media into many aspects of its operational mission, CBP aims to further enable and empower its officers, agents, and analysts to further integrate social media throughout their operational functions. (b) (5)

[Redacted]

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

Background:

Social media has become a powerful source of communication and interaction in the past decade and is likely to continue to evolve on a global scale as an integral component of individual identity. Increases in social media usage and connectivity -- as well as in the prevalence of mobile devices and their enabling of near-constant access to social media platforms -- have enabled adversaries to use social media platforms for their recruitment, communications, strategy, and operations threatening national and border security.

- In March 2014, the CBP Deputy Commissioner directed the [Redacted] (b) (7)(E) [Redacted] (b) (7)(E) (b) (5) [Redacted].
- Subsequent [Redacted] (b) (7)(E) conducted market research, identified a suite of social media tools to support CBP's various functions, (b) (7)(E) [Redacted]

Submitted by: [Redacted] (b) (6), (b) (7)(C)
Date: 6 OCT 2016

INFORMATION ISSUE PAPER

- In December 2015, the CBP Deputy Commissioner directed the formation of a CBP-wide working group designed to assess CBP's current social media operational use footprint and prepare a strategy for advancing those capacities in full consideration of legal, privacy, and civil rights and civil liberties equities.

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

Future Actions: (b) (5)

, CBP assesses that future developments in the use of social media (b) (7)(E) must be made incrementally and responsibly in the face of extremely complex and difficult technological constraints and legal considerations. (b) (7)(E)

(b) (7)(E)

(b) (7)(E)

and significant legal and privacy considerations must be considered in all future developments.

Subsequently, CBP will continue to test and develop new capabilities (b) (7)(E)

in a deliberate and responsible manner (b) (5), (b) (7)(E)

. To this end, CBP has:

- Prepared a Social Media Strategy (b) (5);
- Worked extensively, both with the Department's Social Media Task Force and independently, to assess the efficacy of industry-leading Commercial-off-the-Shelf tools that claim to support the use of social media (b) (7)(E); and,
- Allocated funds to develop agency-wide training programs on the safe, effective, and legal use of social media in support of CBP's screening/vetting responsibilities and the use of social media in (b) (7)(E).

In FY 17, CBP will:

- Begin to deploy developed training across the agency, to include providing industry-leading advanced training to our most experienced and critical users;
- Develop position descriptions and allocate funds to hire full-time staff from the private sector to support developments in this space;

Submitted by: (b) (6), (b) (7)(C)

Date: 6 OCT 2016

INFORMATION ISSUE PAPER

- Execute (b) (7)(E) a series of pilot programs assessing new tools and technology (b) (7)(E);
- Implement lessons learned to date into the workflow of NTC screening/vetting, as appropriate based on technological and legal constraints;
- Begin to make strategic investments in emerging technologies of value in this space;
- (b) (5), (b) (7)(E)

Watch Out For/If Asked:

Is CBP currently using social media information to support (b) (7)(E) ?

- CBP is working with the DHS Social Media Task Force and DHS Oversight bodies in order to address the specific challenges associated with (b) (7)(E), (b) (5)

Does CBP provide social media training to its officers, agents and analysts?

- In order to further incorporate open source collection and social media information into its various operational missions to the extent allowable by law and technologically feasible, CBP empowers its operators to conduct successful social media research through the establishment of and support for consistent training and education programs.
- CBP currently provides introductory and operational security awareness social media training to any CBP employees who use social media for operational purposes.
- (b) (5)

Is there validity to the claim that a Social Media Center of Excellence will be formed/founded at the NTC?

- CBP is currently participating in the DHS Social Media Task Force chaired by the Under Secretary for Intelligence and Analysis to support the creation, in a controlled, thorough, and cost efficient manner, of a social media vetting capability for the Department. Social media has become a powerful source of communication and interaction in the past decade and continues to evolve on a global scale. Increases in

Submitted by: (b) (6), (b) (7)(C)

Date: 6 OCT 2016

INFORMATION ISSUE PAPER

social media usage and connectivity have enabled adversaries to use social media platforms for their recruitment, communications, strategy, and operations threatening national and border security. The concept of a DHS Social Media Center of Excellence recognizes the need to keep pace with these real world requirements by centralizing DHS's technology capabilities, authorities, and policy decisions, and empower its members – without necessarily requiring a brick and mortar COE in one centralized location.

Submitted by: (b) (6), (b) (7)(C)

Date: 6 OCT 2016

USCBP000004

U.S. Customs and Border Protection

(b) (7)(E)

Use of Social Media

May 25, 2016

(U//FOUO) Social media has become a powerful source of communication and interaction in the past decade and is likely to continue to evolve on a global scale as an integral component of individual identity. Increases in social media usage and internet connectivity -- as well as in the prevalence of mobile devices and their enabling of near-constant access to social media platforms -- have created a myriad of new opportunities for national security adversaries or border security threats to use social media platforms for their recruitment, communications, strategy, and operations. As John Carlin, Assistant Attorney General for National Security, said on March 1, 2016, "groups like the Islamic State of Iraq and the Levant (ISIL) are using popular social media platforms to propagate and recruit with greater efficiency than ever before... in addition to a prolific presence on media outlets [e.g., Twitter or Facebook]... well-produced propaganda has become a norm when it comes to drawing outsiders to their cause... what we're seeing is a group that's taking advantage of western-made technology." Subsequently, Social Media has become a critical element for vetting travelers by U.S. Customs and Border Protection (CBP)

(U//FOUO) The collection and screening of social media is (b) (7)(E)

(b) (7)(E)

(b) (7)(E) The information provided in social media is critical to screening for imminent and emergent threats to the United States from travelers who are enabled through social media to recruit, plan, and execute terrorist acts via real-time communication platforms. It is critical that social media information be made available to CBP immediately, not several months from now, in order to prevent, disrupt, and dismantle current terrorist plans, rather than react to them after it is too late. It would be unacceptable to the American Public for the Department to miss an opportunity to disrupt a terrorist act when information is readily available to support more robust screening.

(U//FOUO/LES) CBP will conduct (b) (7)(E) social media (b) (7)(E) to screen for indicators that warrant further review by a law enforcement officer. (b) (7)(E)

(b) (7)(E)

The reviewing officer will use social media information as a tool for vetting travelers to supplement all other available information, (b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(U//FOUO/LES) During social media screening, there may be instances where it is appropriate and necessary to (b) (7)(E)

(b) (7)(E)

to adjudicate a (b) (7)(E)

on

behalf of the traveler.

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E) Social media will never be the sole source of information used for vetting. (b) (7)(E)

(b) (7)(E)

(b) (7)(E) and a case by case basis determination will be made on appropriate enforcement action based on the totality of the circumstances, such as (b) (7)(E)

(b) (7)(E)

(b) (7)(E) Similar to current procedures when

(b) (7)(E)

(b) (7)(E) CBP would only share information on (b) (7)(E) (b) (7)(E) and law enforcement partners that is necessary to complete the mission. All these efforts add to the layered vetting approach to help ensure process oversight.

(U//FOUO/LES) As mentioned above, (b) (7)(E)

(b) (7)(E) CBP assesses the totality of the circumstances in each case, (b) (7)(E)

(b) (7)(E) and an independent determination would be made on each individual case following a thorough vetting. (b) (7)(E)

(b) (7)(E)

(U//FOUO/LES) There are numerous examples of incidents in which (b) (7)(E)

(b) (7)(E)

(b) (7)(E) With the increased number of VWP travelers for the upcoming summer season, it is imperative that the social media collection not be delayed to ensure thorough vetting. (b) (7)(E)

(b) (7)(E)

(U//FOUO) The ability to collect and review social media is not only imperative due to ongoing threats from terrorist organizations, but it is also critical to providing a complete picture of an ESTA applicant. More completely developing this picture leads to numerous (b) (7)(E) benefits, as highlighted above, but also to significant benefits for many travelers as well. For one, collecting social media incorporates into CBP's adjudication process information that would not be otherwise available and can often help resolve identities and clarify information. (b) (7)(E)

[REDACTED]

Therefore, social media serves not only as a vital screening tool and additional selector for vetting, but it also provides the direct benefit to the applicant in entity resolution and application support. In many circumstances, CBP will be unable to meet the statutory requirements of the VWP Act to determine the national security or law enforcement interests of the United States without access to social media information that is collected through the Electronic System for Travel Authorization (ESTA). As stated by Secretary Johnson, "Social media can provide the Department with critical information related to the execution of our mission."

Office of Field Operations

(b) (7)(C), (b) (7)(E)

Use of Social Media

September 26, 2016

Executive Summary:

(U//FOUO/LES) The Visa Waiver Program (VWP) Improvement and Terrorist Travel Prevention Act (The VWP Act) of 2015 established new travel and dual nationality restrictions for VWP applicants. The restrictions include presence after March 1, 2011 in Iran, Iraq, Sudan, Syria, Libya, Somalia or Yemen and dual nationality with Iran, Iraq, Sudan and Syria. The VWP Act also included a provision that allows the Secretary of Homeland Security to waive VWP ineligibilities created by the VWP Act, if the Secretary determines such a waiver is in the law enforcement or national security interests of the United States. The (b) (7)(E) was created to leverage the additional information being collected under the VWP to (b) (7)(E)

The (b) (7)(E) has developed a process for vetting and research of ESTA applications (b) (7)(E)

(b) (7) currently reviews ESTA applications with (b) (7)(E)

(b) (7)(E)

(b) (7)(E)

Social media and open source information (b) (7)(E) details regarding the applicant that may not available through other sources.

Social Media Use in the Electronic System for Travel Authorization

(U) All prospective Visa Waiver Program (VWP) travelers are required to submit biographic identifiers through the online Electronic System for Travel Authorization (ESTA) application. ESTA is the primary means of obtaining identifying information to vet against counterterrorism and law enforcement databases for prospective inbound VWP travelers.

(U//FOUO) The Department of Homeland Security (DHS) is seeking to add an optional data field requesting social media identifiers (or “handles”) from foreign nationals applying for an ESTA.¹ CBP published a proposed change to the ESTA application and I-94W in the Federal Register to add an optional field for applicants to enter their social media handle and provider/platform. CBP has already responded to public comments from the 60-day comment period and provided an additional 30 days for comments.

Current Social Media Use:

¹ It will remain optional, as not every applicant may use social media.

(U//FOUO/LES)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E) vetting may be conducted concurrently and will be used collectively to support an informed decision process. Social media and open source is used in a multitude of ways during the vetting process to (b) (7)(E)

(b) (7)(E)

As mentioned above, DHS proposed additional changes to the ESTA application to allow the applicant to provide a social media platform (e.g. Twitter, Facebook, etc.) and the related identifier (i.e. username, screen name, handle). These changes are currently in the public comment period.

Threat Environment

(U//FOUO/LES)

(b) (7)(E)

(b) (7)(E)

(U//FOUO/LES) Terrorist groups including the Islamic State of Iraq and the Levant (ISIL), al-Qa'ida, and al-Qa'ida's affiliates use social media to disseminate official messaging, recruit potential members, and convince potential supporters to mobilize to violence. (b) (7)(E)

(U//FOUO) DHS is concerned about the thousands of European foreign fighters-as cited in the media. (b) (7)(E)

(U//FOUO) (b) (7)(E)

(b) (7)(E) This information is particularly important to combat a timely, unexpected, and credible threat to public safety.

(U//FOUO) Allowing ESTA applicants to voluntarily share their social media identifiers on their applications (b) (7)(E)

Applicability to Waiver Authority

(U//FOUO) Social media serves not only as a vital screening tool (b) (7)(E) but it also provides the direct benefit to the applicant in entity resolution and application support. (b) (7)(E)

(U//FOUO) Collecting social media incorporates into CBP’s adjudication process information that would not be otherwise available and can often help resolve identities and clarify information. (b) (7)(E)

Social Media Pilot:

(U//FOUO//LES) Social media screening will be done in two ways, in compliance with DHS and CBP policies and directives regarding social media. Social media platforms and the definition of “derogatory information” are constantly evolving, so specific procedures for every scenario would not be possible. However, in general, (b) (7)(E)

(b) (7)(E)

- 1) (b) (7)(E)
- 2) (b) (7)(E)

(b) (7)(E)

~~FOR OFFICIAL USE ONLY~~

(U//FOUO//LES) As it does today, CBP will review the totality of the information available (b) (7)(E) prior to making a determination regarding a person's ESTA application. It is possible that information (b) (7)(E)

(b) (7)(E)

(b) (7)(E) If the ESTA is approved or the waiver is granted, the person will be able to travel to the United States under the VWP. If either are denied, the individual must apply for a visa to travel to the United States.³

(U//FOUO//LES) (b) (7)(E)
(b) (7)(E)

(U//FOUO//LES) (b) (7)(E)
(b) (7)(E)
○ (b) (7)(E)
○
○
○

(U//FOUO//LES) (b) (7)(E)
(b) (7)(E)
○ (b) (7)(E)
○

DHS Science and Technology (S&T)

(U//FOUO//LES) (b) (7)(E) is currently piloting (b) (7)(E) using ESTA application data. (b) (7)(E)

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

³ The denial of an ESTA does not prohibit travel to or admission into the United States.

~~FOR OFFICIAL USE ONLY~~

~~FOR OFFICIAL USE ONLY~~

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

Future State for Social Media:

(U//FOUO/LES) (b) (7)(E), (b) (5)
(b) (7)(E), (b) (5)

~~FOR OFFICIAL USE ONLY~~

Social Media Briefing Paper

Summary

DHS has been at the forefront among Federal agencies in developing the capability to incorporate social media data in its screening and vetting processes. CBP, along with USCIS and TSA, has been developing, testing, and operationalizing the use of social media.

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

Through this work, CBP and the Department more broadly have advanced our understanding of the challenges in screening non-government maintained databases, including the dynamic nature and magnitude of social media information.

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

Current Social Media Pilots/Operational Use

CBP began a social media pilot using ESTA data in early 2016, with the goal of (b) (7)(E)

(b) (7)(E)

In December 2016, CBP added a voluntary question to the ESTA application to request social media handles, (b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E), (b) (5) CBP is gathering metrics to assess the (b) (7)(E) of social media vetting, as well as the technological and research quality of the tools currently being tested. (b) (7)(E)
(b) (7)(E)

Also of note:

- Collecting (b) (7)(E) allow opportunities for vetting agencies to determine eligibility for travel or immigration benefits and enhance identity resolution before they are allowed into the United States.
 - The enhanced screening and vetting efforts of DHS will include social media, as outlined in the Executive Order 13780, Section 5 report, which identified “high value data” elements that should be part of baseline screening. (b) (5), (b) (7)(E)
 - (b) (5), (b) (7)(E)
 - (b) (5)
 - DHS Privacy conducted a Privacy Compliance Review following CBP’s collection of social media handles. (b) (5)
- (b) (7)(E), (b) (5) (b) (7)(E), (b) (5)

Watch Out For

- (b) (5)

(b) (5)



INFORMATION ISSUE PAPER

Office of Field Operations
National Targeting Center (NTC)
June 2, 2016

Action Required: Information Only

Time Constraint: None

Issue:

CBP currently uses social media information in a limited capacity in support (b) (7)(E)

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

Executive Summary:

Despite incorporating social media into many aspects of its operational mission, CBP aims to further enable and empower its officers, agents, and analysts to further integrate social media throughout their operational functions. (b) (5)

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

Background:

Social media has become a powerful source of communication and interaction in the past decade and is likely to continue to evolve on a global scale as an integral component of individual identity. Increases in social media usage and connectivity – as well as increases in the prevalence of mobile devices and their enabling of near-constant access to social media platforms – have enabled adversaries to use social media platforms for their recruitment, communications, strategy, and operations threatening national and border security.

- In March 2014, the CBP Deputy Commissioner directed the (b) (7)(E) (b) (7)(E) (b) (5).
- Subsequently, (b) (7)(E) conducted market research to identify a suite of social media tools to support CBP's various functions (b) (7)(E)
- In December 2015, the CBP Deputy Commissioner directed the formation of a CBP-wide working group designed to assess CBP's current social media operational-use footprint

Submitted by: (Name of Originator)

Date: (Date Document was Originated)

INFORMATION ISSUE PAPER

and prepare a strategy for advancing those capacities in full consideration of legal, privacy, and civil rights and civil liberties equities.

- (b) (5), (b) (7)(E) [Redacted]

Watch Out For/If Asked:

- Is CBP currently using social media information to support its (b) (7)(E) [Redacted]
 - CBP is working with the DHS Social Media Task and DHS Oversight bodies in order to address the specific challenges associated with (b) (7)(E) [Redacted]
- Does CBP provide social media training to its officers, agents and analysts?
 - In order to further incorporate open source collection and social media information into its various operational missions, to the extent allowable by law and technologically feasible, CBP will empower its operators to conduct successful social media research through the establishment of, and support for, consistent training and education programs.
 - CBP currently provides introductory and operational security awareness social media training to any CBP employees who use social media for operational purposes.
 - (b) (5) [Redacted]

INFORMATION ISSUE PAPER

Office of Field Operations
National Targeting Center (NTC)
August 30, 2016

Action Required: Information Only

Time Constraint: None

Issue: CBP currently uses social media information in a limited capacity in support (b) (7)(E)

(b) (7)(E)

Executive Summary: Despite incorporating social media into many aspects of its operational mission, CBP aims to further enable and empower its officers, agents, and analysts to further integrate social media throughout their operational functions. (b) (5)

(b) (5)

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

Background:

Social media has become a powerful source of communication and interaction in the past decade and is likely to continue to evolve on a global scale as an integral component of individual identity. Increases in social media usage and connectivity -- as well as in the prevalence of mobile devices and their enabling of near-constant access to social media platforms -- have enabled adversaries to use social media platforms for their recruitment, communications, strategy, and operations threatening national and border security.

- In March 2014, the CBP Deputy Commissioner directed the (b) (7)(E) (b) (7)(E) (b) (5).
- Subsequent, (b) (7)(E) conducted market research, identified a suite of social media tools to support CBP's various functions, and (b) (7)(E) (b) (7)(E) (b) (7)(E).
- In December 2015, the CBP Deputy Commissioner directed the formation of a CBP-wide working group designed to assess CBP's current social media operational use footprint and prepare a strategy for advancing those capacities in full consideration of legal, privacy, and civil rights and civil liberties equities.

Submitted by: (b) (6), (b) (7)(C)

Date: 30 AUG 2016

INFORMATION ISSUE PAPER

- (b) (5), (b) (7)(E) [Redacted]

Watch Out For/If Asked:

- Is CBP currently using social media information to support its (b) (7)(E) [Redacted] ?
 - CBP is working with the DHS Social Media Task and DHS Oversight bodies in order to address the specific challenges associated with (b) (7)(E) [Redacted]
- Is CBP using social media to monitor select individuals?
 - No
- Does CBP provide social media training to its officers, agents and analysts?
 - In order to further incorporate open source collection and social media information into its various operational missions to the extent allowable by law and technologically feasible, CBP empowers its operators to conduct successful social media research through the establishment of and support for consistent training and education programs.
 - CBP currently provides introductory and operational security awareness social media training to any CBP employees who use social media for operational purposes.
 - (b) (5) [Redacted]

INFORMATION ISSUE PAPER

Office of Field Operations
National Targeting Center (NTC)
April 20, 2017

Action Required: Information Only

Time Constraint: None

Issue: CBP currently uses social media information in a limited capacity in support (b) (7)(E)

(b) (7)(E)

Executive Summary: (b) (7)(E)

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

Background:

Social media has become a powerful source of communication and interaction in the past decade and is likely to continue to evolve on a global scale as an integral component of individual identity. Increases in social media usage and connectivity -- as well as in the prevalence of mobile devices and their enabling of near-constant access to social media platforms -- have enabled adversaries to use social media platforms for their recruitment, communications, strategy, and operations threatening national and border security.

- In March 2014, the CBP Deputy Commissioner directed the (b) (7)(E) (b) (7)(E) (b) (5)
- Subsequently, (b) (7)(E) conducted market research, identified a suite of social media analysis tools to support CBP's various functions, (b) (7)(E) (b) (7)(E) (b) (7)(E)
- In December 2015, the CBP Deputy Commissioner directed the formation of a CBP-wide working group designed to assess CBP's current social media operational use footprint and prepare a strategy for advancing those capacities in full consideration of legal, privacy, and civil rights and civil liberties equities;
- In January 2016, CBP began to participate in the DHS Social Media Task Force, stood up to assess best practices and technologies for incorporating social media information into Department-wide vetting processes;
- (b) (5)

Submitted by: (b) (6), (b) (7)(C)

Date: 20 April 2017

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

(b) (7)(E)

Pilot Efforts:

CBP is working on or preparing for a variety of pilot efforts in this space, including:

- An ongoing pilot with DHS Science and Technology to test the (b) (7)(E) (b) (7)(E) (b) (7)(E) This pilot has reviewed social media information from approximately 250 ESTA applications to date.
- A pilot utilizing the voluntarily provided social media information collected from the ESTA application;

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

Watch Out For/If Asked:

- Is CBP currently using social media information to support its (b) (7)(E) ?
 - CBP is working with the DHS Social Media Task and DHS Oversight bodies, as well as other Inter-Agency Partners in order to address the specific challenges associated with (b) (7)(E).
- Is CBP using social media to monitor select individuals?
 - No
- Does CBP provide social media training to its officers, agents and analysts?

Submitted by: (b) (6), (b) (7)(C)
Date: 20 April 2017

INFORMATION ISSUE PAPER

- CBP currently provides introductory and operational security awareness social media training to any CBP employees who use social media for operational purposes.

- (b) (5)

Submitted by: (b) (6), (b) (7)(C)
Date: 20 April 2017

USCBP000022



PRIVACY THRESHOLD ANALYSIS (PTA)

This form serves as the official determination by the DHS Privacy Office to identify the privacy compliance requirements for all Departmental uses of personally identifiable information (PII).

A Privacy Threshold Analysis (PTA) serves as the document used to identify information technology (IT) systems, information collections/forms, technologies, rulemakings, programs, information sharing arrangements, or pilot projects that involve PII and other activities that otherwise impact the privacy of individuals as determined by the Chief Privacy Officer, pursuant to Section 222 of the Homeland Security Act, and to assess whether there is a need for additional Privacy Compliance Documentation. A PTA includes a general description of the IT system, information collection, form, technology, rulemaking, program, pilot project, information sharing arrangement, or other Department activity and describes what PII is collected (and from whom) and how that information is used and managed.

Please complete the attached Privacy Threshold Analysis and submit it to your component Privacy Office. After review by your component Privacy Officer the PTA is sent to the Department's Senior Director for Privacy Compliance for action. 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 (b) (7)(E)

[\(b\) \(7\)\(E\)@hq.dhs.gov](mailto:(b) (7)(E)@hq.dhs.gov)

Upon receipt from your component Privacy Office, the DHS Privacy Office will review this form and assess whether any privacy compliance documentation is required. If compliance documentation is required – such as Privacy Impact Assessment (PIA), System of Records Notice (SORN), Privacy Act Statement, or Computer Matching Agreement (CMA) – the DHS Privacy Office or component Privacy Office will send you a copy of the relevant compliance template to complete and return.



Privacy Threshold Analysis (PTA)

Specialized Template for Information Collections (IC) and Forms

The Forms-PTA is a specialized template for Information Collections and Forms. This specialized PTA must accompany all Information Collections submitted as part of the Paperwork Reduction Act process (any instrument for collection (form, survey, questionnaire, etc.) from ten or more members of the public). Components may use this PTA to assess internal, component-specific forms as well.

Form Number: N/A

Form Title: Electronic Visa Update System (EVUS)

Component: Customs and Border Protection (CBP) **Office:** **OFO/APP/EVUS**

IF COVERED BY THE PAPERWORK REDUCTION ACT:

Collection Title: Electronic Visa Update System (EVUS)

OMB Control Number:	1651-0139	OMB Expiration Date:	April 30, 2017
Collection status:	Extension	Date of last PTA (if applicable):	Click here to enter a date.

PROJECT OR PROGRAM MANAGER

Name:	(b) (6), (b) (7)(C)	Title:	Director
Office:	OFO/APP/EVUS	Email:	(b) (6), (b) (7)(C)
Phone:	(b) (6), (b) (7)(C)		

COMPONENT INFORMATION COLLECTION/FORMS CONTACT

Name: (b) (6), (b) (7)(C)



Office:	Office of Trade/RR	Title:	Paperwork Reduction Act Clearance Officer
Phone:	(b) (6), (b) (7)(C)	Email:	(b) (6), (b) (7)(C)

SPECIFIC IC/Forms PTA QUESTIONS

1. Purpose of the Information Collection or Form

- a. Describe the purpose of the information collection or form. *Please provide a general description of the project and its purpose, including how it supports the DHS mission, in a way a non-technical person could understand (you may use information from the Supporting Statement).*
If this is an updated PTA, please specifically describe what changes or upgrades are triggering the update to this PTA.

U.S. Customs and Border Protection (CBP) has a responsibility to balance trade and travel while managing threats to the United States posed by people or cargo entering or exiting the United States. When a nonimmigrant alien applies for a visa to travel to the United States, the validity period of their visa can vary considerably depending on their home country. Some visas remain valid for extended periods of up to ten years. Visas from countries with a longer validity period do not enable the U.S. Government to receive regular updated biographic information or other pertinent information from repeat visitors who travel to the United States multiple times over the life-span of a visa. While longer length visas allow travel to the United States with greater ease, they do not inherently allow the United States to receive updated information over the life-span of the visa.

Given these concerns and considerations, the Department of Homeland Security (DHS) has developed the Electronic Visa Update System (“EVUS”), which provides a mechanism through which information updates can be obtained from nonimmigrant aliens who hold a passport issued by an identified country containing a U.S. nonimmigrant visa of a designated category. By requiring enrollment in EVUS as well as the requirement to update biographic and travel information, CBP is increasing the chances of identifying people who may pose a threat to the United States.

The implementation of EVUS will maintain greater security as it will allow the United States to receive updated traveler information over the life-span of the visa instead of only at the application process.

PTA Update: Collection of Social Media Identifiers

DHS/CBP is expanding the EVUS application to match the previously approved Electronic System for Travel Authorization (ESTA) application and request social media identifiers from all EVUS applicants. DHS/CBP will use social media identifiers to conduct



screening, vetting, and law enforcement checks of EVUS applicants using publicly available information on social media. Terrorist groups, including the Islamic State of Iraq and the Levant (ISIL), al-Qa'ida, and al-Qa'ida's affiliates actively use open media (social media, specifically) to disseminate official messaging, recruit potential members, and convince potential supporters to mobilize to violence. Adding such a question to the EVUS application will provide DHS with greater opportunities to inform a determination of eligibility for travel to the United States.

While this field is optional, all information submitted may be used for national security and law enforcement vetting purposes, and for EVUS eligibility determinations. Should an individual choose to provide his or her social media identifier(s), (b) (7)(E)

(b) (7)(E)

(b) (7)(E) DHS/CBP Officers already use publicly available information, including social media information, as part of the existing EVUS screening and vetting processes. Under no circumstance will DHS/CBP violate any social media privacy settings in the processing of EVUS applications.

As with the collection of social media identifiers on the ESTA application, due to the novel privacy risks surrounding this information collection, the DHS/CBP will employ additional privacy risk mitigation strategies to evaluate this information collection:

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

DHS/CBP will memorialize these requirements in an updated EVUS PIA and SORN.

- b. List the DHS (or component) authorities to collect, store, and use this information. *If this information will be stored and used by a specific DHS component, list the component-specific authorities.*

EVUS data collection falls under authorities provided to DHS by the Immigration and Nationality Act (INA). Specifically, entry and admission authorities.



INA § 214(a)(1) specifically authorizes DHS to prescribe by regulation the conditions for an alien's admission and additionally, aliens' entry into the United States may be limited and conditioned by DHS under INA § 215(a)(1).

Section 214(a)(1) of the INA provides that "[t]he admission to the United States of any alien as a nonimmigrant shall be for such time and under such conditions as the Attorney General may by regulations prescribe...."

An applicant for admission has the burden to prove he or she is clearly and beyond doubt entitled to be admitted and is not inadmissible under section 212 of the INA. INA §§ 240(c)(2), 291; 8 C.F.R. § 235.1(f)(1). Immigration officers determine whether any grounds of inadmissibility apply at the time an alien is inspected. 8 C.F.R. § 235.1(a), (f)(1). Moreover, an officer has the authority to require an alien to state under oath any information sought by an immigration officer regarding the purposes and intentions of the alien in seeking admission, including the alien's intended length of stay, intent to remain permanently, and potential grounds of inadmissibility. INA § 235(a)(5).

INA § 215(a)(1) states "[u]nless otherwise ordered by the President, it shall be unlawful for any alien to depart from or enter or attempt to depart from or enter the United States except under such reasonable rules, regulations, and orders, and subject to such limitations and exceptions as the President may prescribe." INA § 215(a)(1) (emphasis added). Subsequently, the President assigned his functions under INA § 215 with respect to aliens to the Secretary of Homeland Security. Exec. Order No. 13323, 69 Fed. Reg. 241 (Dec. 30, 2003). INA § 215(a)(2) prohibits the transport from or into the United States of individuals for which there is "knowledge or reasonable cause to believe that the departure or entry of such other person is forbidden" by INA § 215. INA § 215(a)(1) provides a basis for denial of entry, provided that restrictions "meet the test of reasonableness." Immigration Laws and Iranian Students, 4A Op. Off. Legal Counsel 133, 140 (1979). Together, INA § 215(a) and DOS visa revocation authorities under INA § 221(i) may permit the Government to require EVUS compliance in advance of travel.

2. Describe the IC/Form



<p>a. Does this form collect any Personally Identifiable Information” (PII¹)?</p>	<p><input checked="" type="checkbox"/> Yes <input type="checkbox"/> No</p>
<p>b. From which type(s) of individuals does this form collect information? (Check all that apply.)</p>	<p><input checked="" type="checkbox"/> Members of the public <input type="checkbox"/> U.S. citizens or lawful permanent residents <input checked="" type="checkbox"/> Non-U.S. Persons. <input type="checkbox"/> DHS Employees <input type="checkbox"/> DHS Contractors <input type="checkbox"/> Other federal employees or contractors.</p>
<p>c. Who will complete and submit this form? (Check all that apply.)</p>	<p><input checked="" type="checkbox"/> The record subject of the form (e.g., the individual applicant). <input type="checkbox"/> Legal Representative (preparer, attorney, etc.). <input type="checkbox"/> Business entity. If a business entity, is the only information collected business contact information? <input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Law enforcement. <input type="checkbox"/> DHS employee or contractor. <input checked="" type="checkbox"/> Other individual/entity/organization that is NOT the record subject. <i>Please describe.</i> The application allows for third parties to submit an EVUS enrollment on behalf of an applicant (e.g. travel agencies, family member)</p>
<p>d. How do individuals complete the form? Check all that apply.</p>	<p><input type="checkbox"/> Paper. <input type="checkbox"/> Electronic. (ex: fillable PDF) <input checked="" type="checkbox"/> Online web form. (available and submitted via the internet)</p>

¹ Personally identifiable information means any information that permits the identity of an individual to be directly or indirectly inferred, including any other information which 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.



	<p><i>Provide link:</i> www.EVUS.gov</p>
<p>e. What information will DHS collect on the form? <i>List all PII data elements on the form. If the form will collect information from more than one type of individual, please break down list of data elements collected by type of individual.</i></p>	
<p>As described in the previously issued PIA and SORN for EVUS, all foreign nationals of designated countries in possession of B1/B2, B1 or B2 visas with a ten year validity, will be required to submit the following information to EVUS:</p> <ul style="list-style-type: none"> • Name (English and Native Language) • Date of Birth • Other Name or Aliases (English and Native Language) • Gender • Travel Document Type • Primary Passport Number – Current, unexpired passport • Passport Number That Holds Visa • Passport Country/Citizenship • Passport Issuance Date • Passport Expiration Date • National ID Number • Visa Foil² Number • City of Birth • Country of Birth • Country of Residence • Parents Name (English and Native Language) • Other Citizenship • Home Address (English and Native Language) • Home Telephone • Cell Phone • Work Telephone • Primary Email • Secondary Email • Employer Name (English and Native Language) 	

² The term “visa foil” refers to the actual physical visa that is affixed into a person’s passport. It is the same as a visa number.



- Employee Address
- Employer City
- Employer State/Province/Region
- Employer Country
- Address While in the United States
- U.S. POC Name
- U.S. POC Address
- U.S. POC Phone Number
- Emergency POC Name
- Emergency POC Phone Number
- Emergency POC Email
- IP Address

PTA update:

CBP is submitting this PTA because DHS/CBP seek to add social media identifiers to the EVUS application to match the same social media collections previously approved for the Electronic System for Travel Authorization (ESTA) application. DHS/CBP seeks to add the following information to the EVUS application:

- Social media identifiers, such as username(s) and platforms used;
- Publicly available information from social media Web sites or platforms

f. Does this form collect Social Security number (SSN) or other element that is stand-alone Sensitive Personally Identifiable Information (SPII)? *Check all that apply.*

- | | |
|---|--|
| <input type="checkbox"/> Social Security number | <input type="checkbox"/> DHS Electronic Data Interchange Personal Identifier (EDIPI) |
| <input type="checkbox"/> Alien Number (A-Number) | <input checked="" type="checkbox"/> Social Media Handle/ID |
| <input type="checkbox"/> Tax Identification Number | <input type="checkbox"/> Known Traveler Number |
| <input checked="" type="checkbox"/> Visa Number | <input type="checkbox"/> Trusted Traveler Number (Global Entry, Pre-Check, etc.) |
| <input checked="" type="checkbox"/> Passport Number | <input type="checkbox"/> Driver's License Number |
| <input type="checkbox"/> Bank Account, Credit Card, or other financial account number | <input type="checkbox"/> Biometrics |
| <input type="checkbox"/> Other. <i>Please list: National ID</i> | |



g. List the <i>specific authority</i> to collect SSN or these other SPII elements.	
See above authorities in 1b.	
h. How will this information be used? What is the purpose of the collection? Describe <i>why</i> this collection of SPII is the minimum amount of information necessary to accomplish the purpose of the program.	
<p>The information collected is used to assess (b) (7)(E) (b) (7)(E). The timely and accurate capture of data, enables visa validation and helps ensure alien compliance with United States law. DHS will use the information collected through EVUS to determine whether (b) (7)(E) (b) (7)(E). Specifically, EVUS will vet non-immigrant applicants who wish to travel to the United States for (b) (7)(E) (b) (7)(E).</p> <p>Specifically regarding the collection of social media identifiers, adding social media data will enhance the existing process, and provide DHS/CBP greater clarity and visibility to (b) (7)(E) by providing an additional tool set which DHS/CBP may use to make better informed eligibility determinations. DHS/CBP's collection of a subject's social media identifiers adds (b) (7)(E) (b) (7)(E).</p>	
i. Are individuals provided notice at the time of collection by DHS (<i>Does the records subject have notice of the collection or is form filled out by third party</i>)?	<input checked="" type="checkbox"/> Yes. There is a security notification that user must agree to prior to proceeding with the enrollment. There are also FAQs and a link to the Privacy Act Statement. <input type="checkbox"/> No.

3. How will DHS store the IC/form responses?	
a. How will DHS store the original, completed IC/forms?	<input type="checkbox"/> Paper. Please describe. Click here to enter text. <input checked="" type="checkbox"/> Electronic. All EVUS records are stored in the EVUS information technology system, which is part of the E-



	<p>Business accreditation boundary. All EVUS information is also replicated into the Automated Targeting System (ATS) and used for vetting, law enforcement, and national security purposes.</p> <p><input type="checkbox"/> Scanned forms (completed forms are scanned into an electronic repository). Please describe the electronic repository.</p> <p>Click here to enter text.</p>
<p>b. If electronic, how does DHS input the responses into the IT system?</p>	<p><input type="checkbox"/> Manually (data elements manually entered). Please describe.</p> <p>Click here to enter text.</p> <p><input checked="" type="checkbox"/> Automatically. Please describe.</p> <p>The traveler enters biographic and travel information into the public facing website which is stored within the EVUS system.</p>
<p>c. How would a user search the information submitted on the forms, <i>i.e.</i>, how is the information retrieved?</p>	<p><input checked="" type="checkbox"/> By a unique identifier.³ <i>Please describe.</i> If information is retrieved by personal identifier, please submit a Privacy Act Statement with this PTA.</p> <p>There are two types of users. The public can access their application information by entering either their enrollment number with their passport number, visa foil number (visa foil refers to the actual physical visa that is affixed into a person's passport) and date of birth or with their passport number, visa foil number, date of birth, surname, first name and country of citizenship. DHS users can access information with a single biographic element or combination of data elements (i. e. passport name, first and last name, foil number).</p> <p>The privacy statement can be accessed on the EVUS web page through this link:</p>

³ Generally, a unique identifier is considered any type of "personally identifiable information," meaning any information that permits the identity of an individual to be directly or indirectly inferred, including any other information which 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.



	<p>https://www.evus.gov/, and clicking on the Privacy Act Statement at the bottom.</p> <p><input type="checkbox"/> By a non-personal identifier. <i>Please describe.</i></p> <p>Click here to enter text.</p>
<p>d. What is the records retention schedule(s)? <i>Include the records schedule number.</i></p>	<p>Enrollment information submitted to EVUS generally expires and is deemed “inactive” two years after the initial submission of information by the enrollee. In the event that a traveler's passport remains valid for less than two years from the date of the EVUS notification of compliance, the EVUS enrollment will expire concurrently with the passport. Information in EVUS will be retained for one year after the EVUS travel enrollment expires. After this period, the inactive account information will be purged from online access and archived for 12 years. At any time during the 15-year retention period (generally 3 years active, 12 years archived) CBP will (b) (7)(E) (b) (7)(E) (b) (7)(E) including EVUS enrollment attempts that are unsuccessful, which will remain accessible for (b) (7)(E) (b) (7)(E) NARA guidelines for retention and archiving of data will apply to EVUS (b) (5) .</p> <p>Records replicated on the unclassified and classified networks will follow the same retention schedule.</p> <p>Payment information is not stored in EVUS, but is forwarded to <i>Pay.gov</i> and stored in CBP's financial processing system, CDCDS, pursuant to the DHS/CBP-018, CDCDS system of records notice.</p> <p>When a traveler's EVUS data is used for purposes of processing his or her application for admission to the United States, the EVUS data will be used to create a corresponding admission record in the DHS/CBP-016 Non-Immigrant Information System (NIIS) (March 13, 2015, 80 FR 13398). This corresponding admission record will be retained in accordance with the NIIS retention schedule, which is 75 years.</p>



<p>e. How do you ensure that records are disposed of or deleted in accordance with the retention schedule?</p>	<p>The system automatically purges records based on retention dates.</p>
<p>f. Is any of this information shared outside of the original program/office? <i>If yes, describe where (other offices or DHS components or external entities) and why. What are the authorities of the receiving party?</i></p>	
<p><input checked="" type="checkbox"/> Yes, information is shared with other DHS components or offices. Please describe.</p> <p>Consistent with DHS’s information sharing mission, information stored in EVUS may be shared with other DHS components that have a need to know of the information to carry out their national security, law enforcement, immigration, intelligence, or other homeland security functions.</p> <p><input checked="" type="checkbox"/> Yes, information is shared <i>external</i> to DHS with other federal agencies, state/local partners, international partners, or non-governmental entities. Please describe.</p> <p>Information stored in EVUS may also be shared with other Federal security and counterterrorism agencies, as well as on a case-by-case basis to appropriate state, local, tribal, territorial, foreign, or international government agencies. DHS completes an information sharing and access agreement with Federal partners to establish the terms and conditions of the sharing, including documenting the need to know, authorized users and uses, and the privacy protections for the data.</p> <p><input type="checkbox"/> No. Information on this form is not shared outside of the collecting office.</p>	





**Homeland
Security**

Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
202 (b) (7)(E)@hq.dhs.gov
www.dhs.gov/privacy

Please include a copy of the referenced form and Privacy Act Statement (if applicable) with this PTA upon submission.



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 7, 2017
Date submitted to DHS Privacy Office:	March 9, 2017
Have you approved a Privacy Act Statement for this form? <i>(Only applicable if you have received a waiver from the DHS Chief Privacy Officer to approve component Privacy Act Statements.)</i>	<input checked="" type="checkbox"/> Yes. Please include it with this PTA submission. <input type="checkbox"/> No. Please describe why not. Click here to enter text.
Component Privacy Office Recommendation: <i>Please include recommendation below, including what existing privacy compliance documentation is available or new privacy compliance documentation is needed.</i>	
(b) (5) [Redacted] [Redacted] [Redacted] [Redacted] [Redacted] [Redacted]	



PRIVACY THRESHOLD ADJUDICATION

(TO BE COMPLETED BY THE DHS PRIVACY OFFICE)

DHS Privacy Office Reviewer:	(b) (6), (b) (7)(C)
PCTS Workflow Number:	(b) (7)(E)
Date approved by DHS Privacy Office:	March 14, 2017
PTA Expiration Date	March 14, 2018

DESIGNATION

Privacy Sensitive IC or Form:	Yes If "no" PTA adjudication is complete.
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 SPII applies. <input checked="" 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"/> Specialized training required. <input type="checkbox"/> Other. Click here to enter text.
DHS IC/Forms Review:	Choose an item.
Date IC/Form Approved by PRIV:	Click here to enter a date.
IC/Form PCTS Number:	Click here to enter text.
Privacy Act Statement:	e(3) statement not required. Previously approved PAS for EVUS still valid.
PTA:	No system PTA required. Click here to enter text.
PIA:	PIA update is required.



	<p>If covered by existing PIA, please list: Click here to enter text. If a PIA update is required, please list: DHS/CBP/PIA-033 Electronic Visa Update System (EVUS)</p>
SORN:	<p>SORN update is required. If covered by existing SORN, please list: Click here to enter text. If a SORN update is required, please list: DHS/CBP-022 Electronic Visa Update System (EVUS) System of Records, September 1, 2016, 81 FR 60371</p>
<p>DHS Privacy Office Comments: <i>Please describe rationale for privacy compliance determination above.</i></p>	
<p>CBP is submitting this Forms-PTA to discuss Electronic Visa Update System (EVUS). CBP is expanding the EVUS application to match the previously approved Electronic System for Travel Authorization (ESTA) application and request social media identifiers from all EVUS applicants. CBP will use social media identifiers to conduct screening, vetting, and law enforcement checks of EVUS applicants using publicly available information on social media.</p> <p>This field is optional on the application, but the information offered may be used for national security and law enforcement vetting purposes, and for EVUS eligibility determinations. CBP Officers already use publicly available information, including social media information, as part of the existing EVUS screening and vetting processes. CBP will abide by all social media privacy settings in the processing of EVUS applications.</p> <p>The specific questions CBP wishes to add</p> <ul style="list-style-type: none"> • Social media identifiers, such as username(s) and platforms used; and • Publicly available information from social media Web sites or platforms. <p>The DHS Privacy Office finds that the EVUS initiative is privacy-sensitive requiring both PIA and SORN coverage. Both a PIA Update and an updated SORN to the following artifacts is required.</p> <ul style="list-style-type: none"> • DHS/CBP/PIA-033 Electronic Visa Update System (EVUS) • DHS/CBP-022 Electronic Visa Update System (EVUS) System of Records 	



Homeland Security

Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
202 (b) (7)(E)@hq.dhs.gov
www.dhs.gov/privacy

Please note, the PIA Update must be signed by the Chief Privacy Officer and the updated SORN must clear OMB and be published in the Federal Registrar before the social media questions can be put into operation.

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 requirement¹:

- 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.

¹Gathering 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: 09/18/2015

Name of Component: Customs and Border Protection

Contact Information: (b) (6), (b) (7)(C)

Counsel²Contact Information: (b) (6), (b) (7)(C) Office of Chief Counsel, Enforcement Section

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

- Joint Integrity Case Management System (JICMS),
- Integrated Security Management System (ISMS).

Applicable Privacy Impact Assessment(s) (PIA):

- DHS/ALL/PIA-038(a), [Integrated Security Management System Update](#) September 16, 2014,
- JICMS PIA is currently being drafted

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

- [DHS/ALL-020 - Department of Homeland Security Internal Affairs](#) April 28, 2014, 79 FR 23361

²Counsel 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 are Office of Internal Affairs Investigative Operations Division and Credibility Assessment Division personnel. This SMOUT encompasses using (b) (7)(E)

(b) (7)(E) All allegations against CBP employees are entered through the Joint Intake Center (JIC) process. The CBP Office of Internal Affairs (IA) JIC and Investigative Operations Division (IOD) vets those allegations to determine whether any allegation of corruption and other misconduct rise to the level of criminal conduct. For those allegations determined by Management to be criminal in nature, IA requires the use of

(b) (7)(E)

(b) (7)(E) some of which may be Personally Identifiable Information (PII), per DHS Instruction 110-01-001, Section IV E), in publicly accessible/non-privacy restricted social media forums. This publically accessible/non-privacy restricted information has the potential to (b) (7)(E)

(b) (7)(E)

CBP IA will use social media to (b) (7)(E)
(b) (7)(E) IA will not be involved in the gratuitous gathering of personal social media information or PII. IA does not collect or store as evidence any social media information that is solely an exercise of political speech. IA's focus is solely on identifying information that is (b) (7)(E)

(b) (7)(E)

Once an individual is the subject of a criminal investigation, IA will use social media to

(b) (7)(E)

(b) (7)(E) The information is stored in the Joint Integrity Case Management System is the IT system, which is covered under the DHS/ALL-20- Internal Affairs SORN.

(Note: While some IA investigations are clearly administrative, based on a lack of correlation between [REDACTED]

(b) (7)(E)

(b) (7)(E)

This change in the character of the investigation is a function of prosecutorial discretion, and not an arbitrary decision on the part of IA. Once prosecution of the matter is declined, IA will conduct any further investigation of the matter pursuant to the Internal Affairs Non-Criminal Investigation SMOUT.

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

Authorities to conduct [REDACTED] (b) (7)(E) for criminal investigations includes Title 19 of the U.S. Code, including but not limited to 19 U.S.C. §§ 1589a and 2081, 8 U.S.C. § 1363a (criminal investigations for immigration violations) and by virtue of the Commissioner’s Delegation Order (Customs Order No. 09-007), Section 287 of the Immigration and Nationality Act and its implementing regulations regarding enforcement authorities and responsibilities. See 8 CFR 287.2 (initiating criminal investigation for immigration violations); 8 CFR 287.4 (issue subpoenas in criminal or civil investigations); 8 CFR 287.9 (obtaining search warrant prior to conducting a search in a criminal investigation). Additionally, as of September 18, 2014, the Secretary delegated authority to CBP IA to investigate its employees for alleged criminal misconduct. See also CBP Directive No. 2130-016, “Roles and Responsibilities for Internal Affairs Activities and Functions” (December 23, 2008) and CBP Delegation Order 09-007 “Authority to Designate Federal, State, Local, Tribal and Foreign Law Enforcement Officers as “Customs Officers”; Customs Officer Authority, Immigration Officer Authority (December 21, 2009).

Has Counsel listed above reviewed these authorities for privacy issues and determined that they permit the Program to use social media for the listed operational use?

Yes.

No.

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

In development.

Operational. Date first launched: 10/1/2004

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

Attached. Also attached is the CBP Directive for Operational Use of Social Media, Section 5

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;

Yes. No. If not, please explain:

When IA investigators are conducting a criminal investigation, they may (as is common law enforcement practice in analogous situations) (b) (7)(E)

(b) (7)(E) This being said, the viewing of publically available information/non-privacy restricted social media information may require no interaction with the individual under investigation, so the

(b) (7)(E)

Yes- When CBP uses (b) (7)(E) CBP personnel do not log in, so no profile is created.

No- When Office of Internal Affairs Investigative Operations Division and Credibility Assessment Division personnel conduct limited (b) (7)(E) on social media sites, they need to

(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;

Yes. No. If not, please explain:

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

Yes. No. If not, please explain:

- 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:

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. If not, please explain:

DHS SOCIAL MEDIA DOCUMENTATION
(To be Completed by the DHS Privacy Office)

DATE reviewed by the DHS Privacy Office: January 28, 2016

NAME of the DHS Privacy Office Reviewer (b) (6), (b) (7)(C)

DESIGNATION

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.

Incomplete privacy compliance documentation.

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. DHS/ALL-020 - Department of Homeland Security Internal Affairs April 28, 2014, 79 FR 23361

DHS PRIVACY OFFICE COMMENTS

The DHS Privacy Office finds that CBP's operational use of social media for internal affairs criminal investigations purposes is consistent with their internal affairs investigatory authorities. CBP Internal Affairs has authority to conduct investigations using open source, publicly available information from social media as they would any other type of publicly available information collection. We also agree that due to the nature of their investigatory needs, they may (b) (7)(E)

(b) (7)(E)

(b) (7)(E)

CBP IA must still follow all other standard

rules of behavior.

However, the DHS Privacy Office also finds that the compliance documentation for this program is incomplete and requires an immediate update. CBP must complete the (b) (5) [REDACTED]. In addition, DHS will update the DHS/ALL-020 Internal Affairs SORN to more clearly represent open source social media as a category of records and record source.

These outstanding compliance requirements must be completed within six months (July 28, 2016).

PCTS # (b) (7)(E)



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 (b) (7)(E)

(b) (7)(E)@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:

(b) (7)(E)@hq.dhs.gov, phone: 202-(b) (7)(E)



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 (b) (4), (b) (7)(E) 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)



<p><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>	<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
--	--

<p>4. What specific information about individuals is collected, generated or retained?</p>	
<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: (b) (4), (b) (7)(E) 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) (5), (b) (7)(E)	
[REDACTED]	
[REDACTED]	
[REDACTED]	
[REDACTED]	
[REDACTED]	
[REDACTED]	
[REDACTED]	
[REDACTED]	

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.

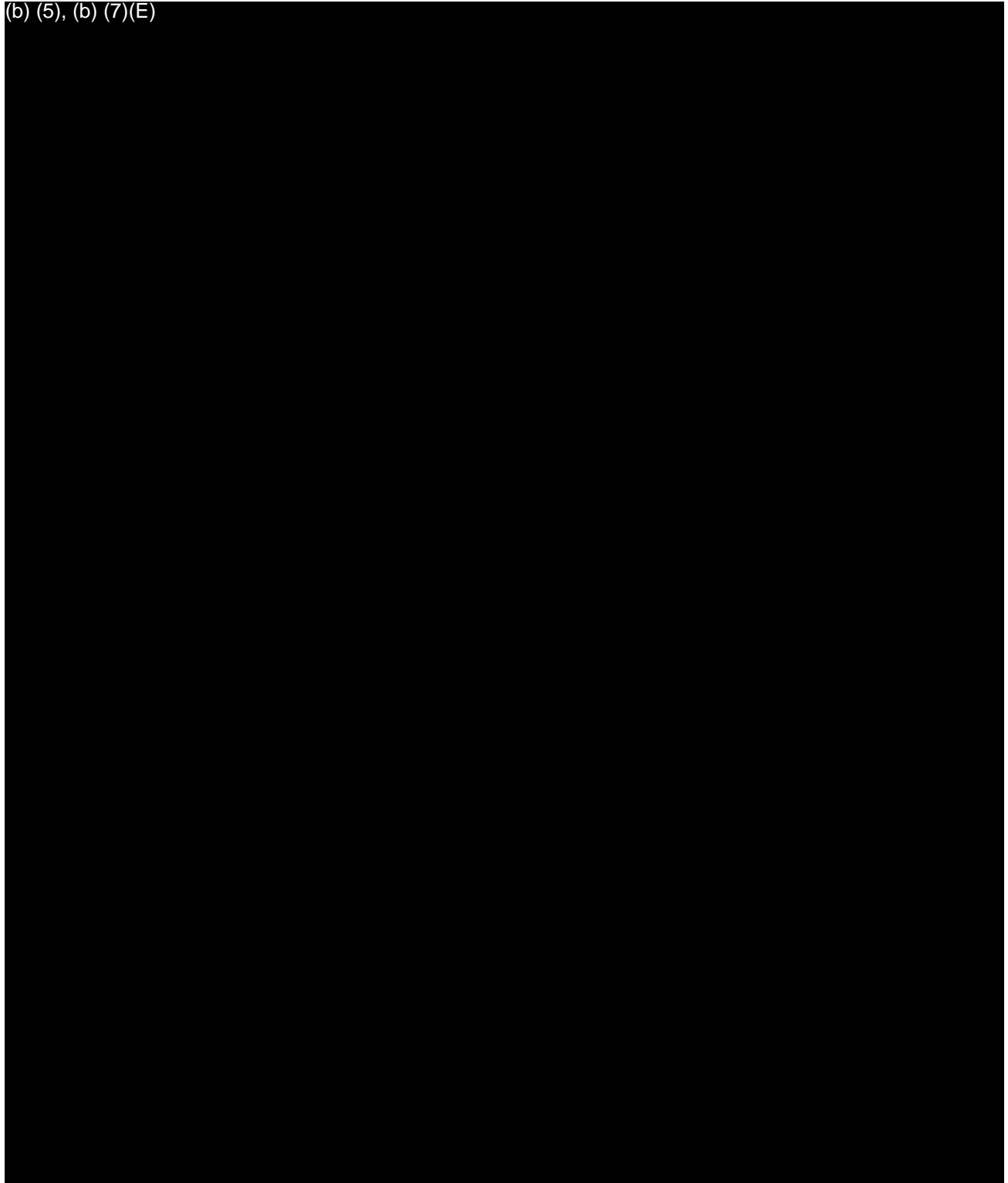


**Homeland
Security**

Privacy Office
U S Department of Homeland Security
Washington, DC 20528
202 (b) (7)(E)@dhs.gov
www.dhs.gov/privacy

Privacy Threshold Analysis
Version number: 01-2014
Page 8 of 10

(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:	(b) (7)(E)
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.