

Exhibit A

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) [Redacted]

Future Actions: (b) (5) [Redacted], CBP assesses that future developments in the use of social media (b) (7)(E) [Redacted] must be made incrementally and responsibly in the face of extremely complex and difficult technological constraints and legal considerations. (b) (7)(E) [Redacted] 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) [Redacted] in a deliberate and responsible manner (b) (5), (b) (7)(E) [Redacted]. To this end, CBP has:

- Prepared a Social Media Strategy (b) (5) [Redacted];
- 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) [Redacted]; 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) [Redacted].

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) [Redacted]
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.
- CBP is in the process of establishing (b) (7)(E) training curriculum.

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

Unclassified//For Official Use Only/Law Enforcement Sensitive

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)

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)

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

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

to adjudicate a (b) (7)(E) on behalf of the traveler. (b) (7)(E)

(Unclassified//For Official Use Only/Law Enforcement Sensitive)

USCBP000005

Unclassified//For Official Use Only/Law Enforcement Sensitive

(b) (7)(E)

Social media will never be the sole source of information used for vetting.

(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)

Similar to current procedures when

(b) (7)(E)

CBP would only share information on 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)

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

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

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

(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)

Unclassified//For Official Use Only/Law Enforcement Sensitive

(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."

(Unclassified//For Official Use Only/Law Enforcement Sensitive)

USCBP000007

FOR OFFICIAL USE ONLY

Office of Field Operations

(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)(E) currently reviews ESTA applications with (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.

FOR OFFICIAL USE ONLY

(U//FOUO//LES) (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)

(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)

FOR OFFICIAL USE ONLY

(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)

1)

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)

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)

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

(U//FOUO//LES) (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)

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

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)

UNCLASSIFIED//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)

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

UNCLASSIFIED//FOR OFFICIAL USE ONLY

(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. CBP is leveraging the RAND Corporation for an external assessment and red-teaming efforts to support CBP's analysis.

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) (5)

Watch Out For

- (b) (5)

UNCLASSIFIED//FOR OFFICIAL USE ONLY

UNCLASSIFIED//FOR OFFICIAL USE ONLY

(b) (5)



UNCLASSIFIED//FOR OFFICIAL USE ONLY

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) (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) (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)

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.
 - CBP is in the process of formalizing (b) (7)(E)
[REDACTED] training curriculum.

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

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 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?
 - 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.
 - CBP is in the process of establishing (b) (7)(E) training curriculum.

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), (b) (5)

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

INFORMATION ISSUE PAPER

- (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) [redacted]. 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) [redacted] ?
 - 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) [redacted].
- 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) [redacted]
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.
- CBP is in the process of formalizing [REDACTED] (b) (7)(E) [REDACTED] training curriculum.



**Homeland
Security**

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

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: 202-343-1717

PIA@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) | | |
| Office: | OFO/APP/EVUS | Title: | Director |
| Phone: | (b) (6), (b) (7)(C) | Email: | (b) (6), (b) (7)(C) @cbp.dhs.gov |

COMPONENT INFORMATION COLLECTION/FORMS CONTACT

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



Homeland Security

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

| | | | |
|---------|---------------------|--------|---|
| Office: | Office of Trade/RR | Title: | Paperwork Reduction Act Clearance Officer |
| Phone: | (b) (6), (b) (7)(C) | Email: | (b) (6), (b) (7)(C)@cbp.dhs.gov |

OV

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



Homeland Security

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

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)

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.



Homeland Security

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

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



Homeland Security

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

| | |
|---|--|
| <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.



Homeland Security

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

Provide link:
www.EVUS.gov

e. What information will DHS collect on the form? *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.*

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:

- 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.



Homeland Security

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

- 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> | |



Homeland Security

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

| | |
|---|--|
| <p>g. List the specific authority to collect SSN or these other SPII elements.</p> <p>See above authorities in 1b.</p> | |
| <p>h. How will this information be used? What is the purpose of the collection? Describe why this collection of SPII is the minimum amount of information necessary to accomplish the purpose of the program.</p> <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). Specifically, EVUS will vet non-immigrant applicants who wish to travel to the United States for (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).</p> | |
| <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>)?</p> | <p><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.</p> <p><input type="checkbox"/> No.</p> |

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



Homeland Security

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

| | |
|--|--|
| | <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.



Homeland Security

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

| | |
|--|---|
| | <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 match data linked to active law enforcement lookout records to enforcement activities, and/or investigations or cases, including EVUS enrollment attempts that are unsuccessful, which will remain accessible for the life of the law enforcement activities to which they may become related. NARA guidelines for retention and archiving of data will apply to EVUS (b) (5) [REDACTED].</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> |



Homeland Security

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

| | |
|--|--|
| <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
202-343-1717, pia@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.



Homeland Security

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

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] | |



Homeland Security

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

PRIVACY THRESHOLD ADJUDICATION

(TO BE COMPLETED BY THE DHS PRIVACY OFFICE)

| | |
|--------------------------------------|---------------------|
| DHS Privacy Office Reviewer: | (b) (6), (b) (7)(C) |
| PCTS Workflow Number: | 1140114 |
| 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. |



Homeland Security

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

| | |
|--|--|
| | <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
202-343-1717, pia@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.



**Homeland
Security**

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

Privacy Threshold Analysis
Version number: 01-2014
Page 1 of 10

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.



Homeland Security

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

Privacy Threshold Analysis
Version number: 01-2014
Page 2 of 10

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 |



Homeland Security

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

Privacy Threshold Analysis
Version number: 01-2014
Page 3 of 10

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)



Homeland Security

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

Privacy Threshold Analysis
Version number: 01-2014
Page 4 of 10

| | |
|---|--|
| <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> | <p><input checked="" type="checkbox"/> Web portal³ (e.g., SharePoint)</p> <p><input type="checkbox"/> Contact Lists</p> <p><input type="checkbox"/> None of these</p> |
|---|--|

| | |
|---|--|
| <p>3. From whom does the Project or Program collect, maintain, use, or disseminate information? <i>Please check all that apply.</i></p> | <p><input type="checkbox"/> This program does not collect any personally identifiable information⁴</p> <p><input checked="" type="checkbox"/> Members of the public</p> <p><input checked="" type="checkbox"/> DHS employees/contractors (list components):</p> <p><input checked="" type="checkbox"/> Contractors working on behalf of DHS</p> <p><input type="checkbox"/> Employees of other federal agencies</p> |
|---|--|

| |
|---|
| <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.



Homeland Security

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

Privacy Threshold Analysis
Version number: 01-2014
Page 5 of 10

(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.”

| | |
|---|---|
| <p>4(a) Does the project, program, or system retrieve information by personal identifier?</p> | <p><input checked="" type="checkbox"/> No. Please continue to next question. <input type="checkbox"/> Yes. If yes, please list all personal identifiers used:</p> |
| <p>4(b) Does the project, program, or system use Social Security Numbers (SSN)?</p> | <p><input checked="" type="checkbox"/> No. <input type="checkbox"/> Yes.</p> |
| <p>4(c) If yes, please provide the specific legal basis and purpose for the collection of SSNs:</p> | <p>Click here to enter text.</p> |
| <p>4(d) If yes, please describe the uses of the SSNs within the project, program, or system:</p> | <p>Click here to enter text.</p> |
| <p>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></p> | <p><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.</p> |



Homeland Security

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

Privacy Threshold Analysis
Version number: 01-2014
Page 6 of 10

| |
|---|
| 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.



Homeland Security

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

Privacy Threshold Analysis
Version number: 01-2014
Page 7 of 10

| | |
|---|---|
| <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) | |
| [Redacted] | |
| [Redacted] | |
| [Redacted] | |
| (b) (7)(E), (b) (5) | |
| [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.



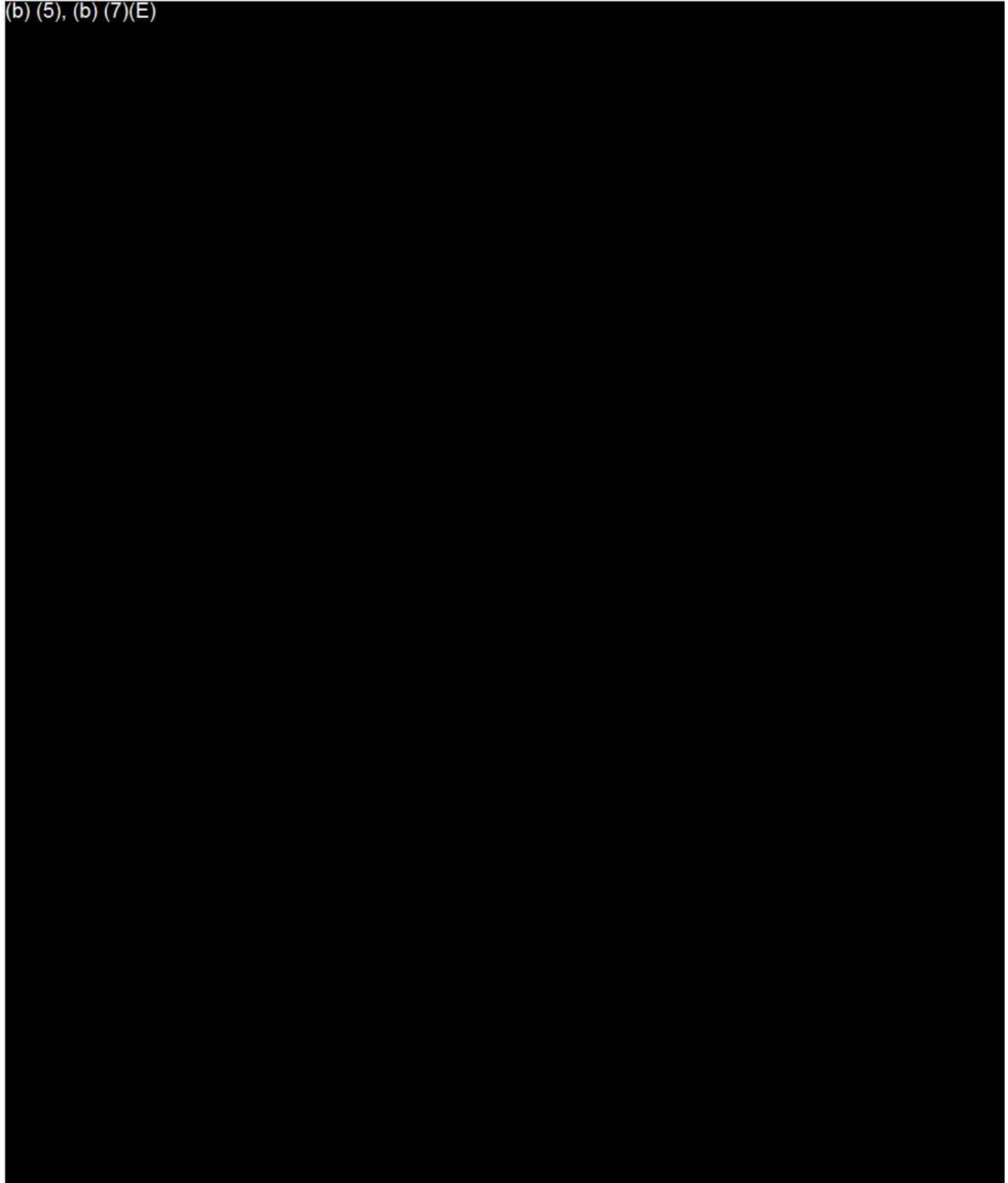
Homeland Security

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

Privacy Threshold Analysis
Version number: 01-2014

Page 8 of 10

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





Homeland Security

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

Privacy Threshold Analysis
Version number: 01-2014
Page 9 of 10

| |
|--|
| |
|--|

(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 |



Homeland Security

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

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

| | |
|---|---|
| | <p>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</p> |
| <p>DHS Privacy Office Comments: <i>Please describe rationale for privacy compliance determination above.</i></p> | |
| <p>CBP is submitting this PTA to discuss its use of the (b) (7)(E) in a testing and evaluation pilot. (b) (7)(E)</p> | |
| <p style="text-align: center; font-size: 2em; font-weight: bold;">(b) (7)(E)</p> | |
| <p>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.</p> | |
| <p>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.</p> | |
| <p>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.</p> | |
| <p>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.</p> | |
| <p>(b) (5), (b) (7)(E)</p> | |
| <p>This PTA expires in 3 years.</p> | |

U.S. CUSTOMS AND BORDER PROTECTION DIRECTIVE

CBP DIRECTIVE NO. 5410-003

DATE: January 2, 2015

ORIGINATING OFFICE: OC-PDO

REVIEW DATE: January 2018

SUBJECT: OPERATIONAL USE OF SOCIAL MEDIA

1 PURPOSE

To assign responsibilities and establish general rules of behavior for the operational uses of social media for U.S. Customs and Border Protection (CBP), in compliance with all applicable statutes, regulations, and Department of Homeland Security (DHS) or government-wide policies.

2 SCOPE

This Directive applies to all CBP employees, contractors, and to persons using CBP systems in furtherance of the CBP mission. However, this Directive does not apply to the operational use of social media for communications and outreach with the public authorized by the DHS Office of Public Affairs. Moreover, this Directive does not apply to the operational use of social media to the extent that CBP is utilizing social media for situational awareness purposes on behalf of the DHS National Operations Center.

3 POLICY

It is the policy of CBP to collect, maintain, use, and disseminate PII through the operational use of social media only when there is an authorized need to know the information. CBP will protect PII collected during the authorized operational use of social media, and comply with DHS privacy policy, applicable privacy laws, federal government-wide policies, and other statutory authorities. The procedures set forth in this directive must be followed before PII may be collected by CBP through the use of social media, stored in a CBP system of records, or shared with another party.

4 AUTHORITIES/REFERENCES

- 4.1 Public Law 107-347, "E-Government Act of 2002," as amended, Section 208 [44 U.S.C. § 3501 note];
- 4.2 Title 5, U.S. Code, Section 552a, "Records maintained on individuals" [The Privacy Act of 1974, as amended];
- 4.3 Title 6, U.S. Code, Section 142, "Privacy Officer;"
- 4.4 Title 8, U.S. Code, Section 1363a;

FOUO

- 4.5 Title 19, U.S. Code, Section 2081;
- 4.6 Title 44, U.S. Code, Chapter 35, Subchapter III, "Information Security" [The Federal Information Security Management Act of 2002, as amended (FISMA)];
- 4.7 Title 6, C.F.R., Chapter 1, Part 5, "Disclosure of records and information;"
- 4.8 DHS Delegation 13001, "Delegation to the Chief Privacy Officer;"
- 4.9 DHS Sensitive Systems Policy Directive 4300A;
- 4.10 DHS Directive 047-01 "Privacy Policy and Compliance" (July 7, 2011) and Instruction 047-01-001 "Privacy Policy and Compliance" (July 25, 2011);
- 4.11 DHS Directive 110-01 "Privacy Policy for Operational Use of Social Media" (June 8, 2012) and Instruction 110-01-001 "Privacy Policy for Operational Use of Social Media" (June 8, 2012);
- 4.12 CBP Memorandum "Privacy Compliance and U.S. Customs and Border Protection" (February 10, 2012);
- 4.13 CBP Memorandum "Executive Agent Appointment for a CBP Integrated Intelligence, Surveillance, and Reconnaissance (ISR) Capability" (July 20, 2011);
- 4.14 CBP Information Systems Security Policies and Procedures Handbook 1400-05D; and
- 4.15 CBP Delegation Order 11-001 "Delegation of Authority for Discipline and Adverse Actions" (April 6, 2011).

5 DEFINITIONS

- 5.1 ***Business Owner*** means the CBP employee responsible for the planning and operation of a CBP project, operation, or program that collects PII.
- 5.2 ***Fair Information Practice Principles*** means the policy framework adopted by DHS in Directive 047-01, "Privacy Policy and Compliance," regarding the collection, use, maintenance, disclosure, deletion, or destruction of PII.
- 5.3 ***Individual*** means a natural person, including United States citizens and aliens (e.g., lawful permanent residents and nonimmigrants).
- 5.4 ***Masked Monitoring*** means using identities or credentials on social media that do not identify a DHS/CBP affiliation, or otherwise concealing a government affiliation, to conduct research or general, operational awareness. Masked

FOUO

monitoring includes logging in to social media, but does not include engaging or interacting with individuals on or through social media (which is defined as Undercover Engagement, below).

- 5.5 Operational Awareness** means information gathered from a variety of sources that, when communicated to emergency managers and decision makers, can form the basis for incident management or readiness state decision making.
- 5.6 Overt Research** means collecting information from social media without logging in or otherwise interacting with individuals through social media. Overt research does not include creating identities or credentials on social media, nor does it include concealing a government affiliation to conduct research or general, operational awareness (e.g., non-DHS affiliated IP address).
- 5.7 Overt Engagement** means logging in to social media using DHS/CBP-branded credentials or otherwise indicating an official agency presence and engaging or interacting with individuals on or through social media.
- 5.8 Overt Monitoring** means logging in to social media using DHS/CBP-branded credentials or otherwise indicating an official agency presence, but does not include engaging or interacting with individuals on or through social media (which is defined as Overt Engagement, above).
- 5.9 Operational Use** means use of social media to collect PII for the purpose of enhancing general operational awareness, investigating an individual in a criminal, civil, or administrative context, assist in making a benefit determination about a person, assist in making a personnel determination about a CBP employee or contractor, assist in making a suitability determination about a prospective CBP employee or contractor, or for any other official CBP purpose that has the potential to affect the rights, privileges, or benefits of an individual or CBP employee or contractor. Operational use does not include the use of search engines for general Internet research, the use of social media for professional development (e.g., training and continuing education), or the use of social media for facilitating internal meetings, assigning or trading work shifts, or other internal administrative efficiencies.
- 5.10 Personally Identifiable Information (PII)** means any information that permits the identity of an individual to be directly or indirectly inferred, including other information that is linked or linkable to an individual.
- 5.11 Privacy Compliance Documentation** means any document required by statute or by the Chief Privacy Officer that supports compliance with DHS privacy policy, procedures, or requirements, including but not limited to the Social Media Operational Use Template (SMOUT), Privacy Impact Assessments (PIAs), System of Records Notices (SORNs), Notices of Proposed Rulemaking for Exemption from

certain aspects of the Privacy Act (NPRM), and Final Rules for Exemption from certain aspects of the Privacy Act.

- 5.12 *Privacy Liaison*** means the CBP employee responsible for serving as a point of contact and initial identifier of privacy issues in a CBP office.
- 5.13 *Project Manager*** means the CBP employee or contractor in the Office of Information and Technology or other Office responsible for building and technically maintaining an authorized system with privacy implications.
- 5.14 *Social Media*** means the sphere of websites, applications, and web-based tools that connect users to engage in dialogue, share information and media, collaborate, and interact. Social media take many different forms, including but not limited to web-based communities and hosted services, social networking sites, video and photo sharing sites, blogs, virtual worlds, social bookmarking, and other emerging technologies. This definition does not apply to internal Department intranets or applications.
- 5.15 *Social Media Operational Use Template (SMOUT)*** means the document that each office must submit to the CBP Privacy and Diversity Office for approval by the DHS Privacy Office that describes the current or proposed category of operational uses(s) of social media, identifies the appropriate authorities for the current or proposed category of use(s), describes what PII, if any, is or would be collected (and from whom or by what method), how that information is used, where the information would be stored, and if that collection, storage, and usage is consistent with the current SORN, and any appropriate training. The Template is used to identify information technology systems, technologies, rulemakings, programs, or pilot projects that involve collecting PII from social media for the current or proposed category of use(s) and to assess whether there is a need for additional Privacy Compliance Documentation. Through submission to the CBP Privacy and Diversity Office, templates will be reviewed and adjudicated by the DHS Chief Privacy Officer, and every three years thereafter for accuracy.
- 5.16 *System of Records Notice (SORN)*** means the official public notice of a DHS or CBP system of records as required by the Privacy Act of 1974 (as amended). The SORN identifies (1) the purpose for the system of records, (2) the individuals covered by information in the system of records, (3) the categories of records maintained about individuals, (4) the source of the records and (5) the ways in which the information is generally shared by DHS and CBP. The SORN also provides notice of the mechanisms available for individuals to exercise their Privacy Act rights to access and correct the PII that DHS and CBP maintains about them.
- 5.17 *Undercover Engagement*** means using identities or credentials on social media that do not identify a DHS/CBP affiliation, or otherwise concealing a government affiliation, to engage or interact with individuals on or through social media.

FOUO

6 RESPONSIBILITIES

- 6.1 All CBP employees, contractors, and persons using CBP systems in furtherance of the CBP mission are responsible for:**
 - 6.1.1 Using social media for operational purposes only when activities are authorized by statute, executive order, regulation, or policy and approved through the procedures in this Directive;**
 - 6.1.2 Using only government-issued equipment, internet connections authorized to access social media through the DHS/CBP network (i.e., no “stand-alone” connections), and government-approved accounts when engaging in the operational use of social media, unless otherwise specifically authorized and approved;**
 - 6.1.3 Use screen names or identities that indicate an official DHS/CBP affiliation and use DHS/CBP email addresses to open accounts used when engaging in the operational use of social media, unless otherwise specifically authorized and approved;**
 - 6.1.4 Accessing publicly available information through social media only by reviewing posted information without interacting with any individual who posted the information, unless otherwise specifically authorized and approved;**
 - 6.1.5 Respecting individuals’ privacy settings and access only information that is publicly available unless the individual whose information the employee seeks to access has given consent to access it, or as otherwise authorized and approved;**
 - 6.1.6 Collecting only the minimum PII necessary for the proper performance of their authorized duties;**
 - 6.1.7 Protecting PII as required by the Privacy Act and DHS privacy policy;**
 - 6.1.8 Documenting operational use of social media, including date, site(s) accessed, information collected, and how it was used in the same manner that CBP would document information collected from any source in the normal course of business;**
 - 6.1.9 Complying with DHS Directive 110-01 and Instructions 110-01-001, with privacy policies and procedures issued by the DHS Chief Privacy Officer, and with applicable CBP policies on operational use of social media; and**
 - 6.1.10 Completing training on the operational use of social media and signing the CBP Operational Use of Social Media Rules of Behavior before any social media use and annually thereafter, if operational use of social media is a continuing requirement in the performance of their responsibilities.**

FOUO

6.2 The Assistant Commissioner for the Office of Information and Technology is responsible for:

- 6.2.1 Providing web technology services, security, and technical assistance for the operational use of social media within CBP; and**
- 6.2.2 Ensuring that any technical system providing Masked Monitoring and/or Undercover Engagement accurately documents user login credentials and profiles and maintains sufficient audit logs for each user.**

6.3 The Assistant Commissioner for the Office of Intelligence and Investigative Liaison is responsible for serving as the Business Owner governing the provision of intelligence, surveillance, and reconnaissance (ISR) capabilities, including Masked Monitoring and Undercover Engagement of Social Media. This includes ensuring Masked Monitoring and Undercover Engagement of Social Media meet operational and intelligence needs and providing direction to Office of Information and Technology (OIT) regarding intelligence related technologies available to be leveraged for all aspects of ISR to be used within CBP.

6.4 The CBP Privacy Officer is responsible for:

- 6.4.1 Maintaining an accurate accounting of all CBP categories of operational use of social media using the SMOUT to identify collection and use of PII, the authority for such collection and use, and any other attendant privacy impacts, and ensuring CBP implements DHS privacy policy with respect to the operational use of social media;**
- 6.4.2 Coordinating with CBP Business Owners and Project Managers, as appropriate, together with the DHS Chief Privacy Officer and the Office of Chief Counsel to complete a SMOUT and any other required Privacy Compliance Documentation for (1) for all proposed categories of operational use of social media, and (2) for any changes to the categories of operational use of social media ;**
- 6.4.3 Developing and reviewing CBP policies and directives related to Operational Use of social media, and CBP Rules of Behavior consistent with the adjudicated Template, to ensure compliance with DHS privacy policy, privacy laws applicable to DHS, and federal government-wide privacy policies;**
- 6.4.4 Overseeing CBP privacy training for operational use of social media and providing educational materials, consistent with privacy training for operational use of social media developed by the DHS Chief Privacy Officer;**
- 6.4.5 Reviewing documentation required in 6.1.8 to ascertain compliance with this Directive as needed; and**

FOUO

6.4.6 Collaborating with the DHS Chief Privacy Officer in conducting Privacy Compliance Reviews.

6.5 CBP Office of Chief Counsel is responsible for:

6.5.1 Providing advice to Business Owners or Project Managers, as appropriate, to ensure that appropriate authority exists to engage in categories of operational use of social media before CBP employees engage in those uses, and to ensure that the Template generally documents that authority;

6.5.2 Providing legal guidance to the CBP Privacy Officer, Business Owners, or Project Managers, as appropriate, in the drafting of CBP Operational Use of Social Media Rules of Behavior Rules of Behavior for operational use of social media.

6.6 CBP Business Owners and Project Managers, as appropriate, are responsible for:

6.6.1 Coordinating with the CBP Privacy Officer to ensure that privacy is appropriately addressed when proposing, developing, implementing, or changing any operational use of social media;

6.6.2 Coordinating with the CBP Privacy Officer and the Office of Chief Counsel to prepare draft Templates and CBP Operational Use of Social Media Rules of Behavior, and, as appropriate, all Privacy Compliance Documentation required when proposing, developing, or implementing or changing any category of operational use of social media;

6.6.3 Monitoring the design, deployment, operation, and retirement of programs involving the operational use of social media to ensure that the use of PII, if any, is limited to those uses described in the Privacy Compliance Documentation;

6.6.4 Ensuring oversight mechanisms, including, for example, audit trails and/or privacy compliance reviews, as appropriate, are built into the design of programs and systems involving the operational use of social media;

6.6.5 Coordinating with the CBP Privacy Officer to establish administrative, technical, and physical controls for storing and safeguarding PII consistent with DHS privacy, security, and records management requirements to ensure the protection of PII from unauthorized access, disclosure, or destruction in the course of operational use of social media; and

6.6.6 Supporting the CBP Privacy Officer in developing and implementing privacy procedures and job-related privacy training to safeguard PII in operational uses of social media.

FOUO

7

6.7 Supervisors are responsible for:

6.7.1 Reviewing request(s) for Overt Research of social media, considering the purpose of the request, and determining whether granting approval would serve an appropriate authorized purpose for an operational need that has been approved by the Chief Privacy Officer through a SMOUT; and

6.7.2 Approving or denying such requests.

6.8 Second Level Supervisors, or higher, are responsible for:

6.8.1 Reviewing request(s) for Overt Monitoring, Overt Engagement, and Masked Monitoring of social media, considering the purpose of the request, and determining whether granting approval would serve an appropriate authorized purpose for an operational need that has been approved by the Chief Privacy Officer through a SMOUT; and

6.8.2 Approving or denying such requests.

6.9 Supervisors in the Senior Executive Service, and Second Level Supervisors at the GS-15 Level, or higher, delegated by the Office of Internal Affairs Director of Investigative Operations Division are responsible for:

6.9.1 Reviewing request(s) for Undercover Engagement of social media, considering the purpose of the request, and determining whether granting approval would serve an appropriate authorized purpose for an operational need that has been approved by the Chief Privacy Officer through a Template; and

6.9.2 Approving or denying such requests.

7 PROCEDURES

7.1 General Procedures

7.1.1 Each CBP Office must complete a Template. That Template must identify which parts of the Office engages in operational use of social media, the type of operational use and the purposes achieved through the program(s). This must be completed before engaging in any operational uses of social media, including Overt Research, Overt Monitoring, Overt Engagement, Masked Monitoring, or Undercover Engagement.

7.1.2 The Office must provide the completed Template to the CBP Privacy and Diversity Office via its Privacy Liaison (if the office has a designated Privacy Liaison) or directly to the CBP Privacy Officer.

FOUO

- 7.1.3** The CBP Privacy and Diversity Office, with appropriate coordination with the Office of Chief Counsel, must review and approve the Template before submitting it to the DHS Chief Privacy Officer for review and approval.
- 7.1.4** If directed by the DHS Chief Privacy Officer, the CBP Privacy Officer and the Office must complete any Privacy Compliance Documentation to address the particular operational use of social media stated in the completed Template.
- 7.1.5** The Office must complete any other additional steps outlined in Sections 7.2, 7.3, 7.4, 7.5, or 7.6 of this Directive, as appropriate.
- 7.1.6** Authorized CBP employees, contractors, and persons using CBP systems in furtherance of the CBP mission who plan to use social media under this directive, after a Template is approved, must complete training regarding the Operational Use of social media. These persons must also sign and comply with the CBP Operational Use of Social Media Rules of Behavior before engaging in any of the activities listed in Sections 7.2, 7.3, 7.4, 7.5, or 7.6 of this Directive, and annually thereafter.
- 7.1.7** All CBP employees, contractors, and persons using CBP systems in furtherance of the CBP mission who have created and used social media log-in credentials or profiles for operational use prior to the promulgation of this Directive must submit a request as specified in Sections 7.2, 7.3, 7.4, 7.5, or 7.6 of this Directive and must also complete training and sign the CBP Operational Use of Social Media Rules of Behavior within 90 days of the implementation date of this Directive to continue utilizing the credential or profile.
- 7.1.8** All information collected through social media must be recorded in the appropriate system of records, including date, site(s) accessed, information collected, and how the information was used, in the same manner that CBP would document information collected from any source in the normal course of business. All information collected through social media must be protected in the appropriate system of records to the same extent as other PII in that system and follow any chain of custody requirements for that system, as appropriate.

7.2 Overt Research

- 7.2.1** CBP employees, contractors, and persons using CBP systems in furtherance of the CBP mission must obtain approval from a CBP supervisor before conducting Overt Research of social media.
- 7.2.2** CBP employees, contractors, and persons using CBP systems in furtherance of the CBP mission may conduct Overt Research of social media, after obtaining approval, if the research is necessary for an authorized purpose with a clear nexus to their assigned duties after a properly approved Template is in place.

FOUO

7.3 Overt Monitoring of Social Media

- 7.3.1** CBP employees, contractors, and persons using CBP systems in furtherance of the CBP mission must obtain approval from a second level CBP supervisor, or higher, before Overt Monitoring of social media.
- 7.3.2** Requests for approval for Overt Monitoring of social media must describe the authorized mission, the CBP employees, contractors, and persons using CBP systems in furtherance of the CBP mission authorized to use social media, the nexus to their assigned duties, the social media and any log-in credentials and profile information (including names, email addresses, photographs, etc.) used, and the authority to conduct the program.
- 7.3.3** Approved employees, contractors, and persons using CBP systems in furtherance of the CBP mission must identify themselves as associated with CBP by applying appropriate branding and disclaimers to distinguish the agency's activities from those of nongovernment actors. For example, Business Owners or Project Managers should add the CBP seal or emblem to the program's profile page on a social media website to indicate that it is an official agency presence.

7.4 Overt Engagement of Social Media

- 7.4.1** CBP employees, contractors, and persons using CBP systems in furtherance of the CBP mission must obtain approval from a second level CBP supervisor, or higher, before Overt Engagement of social media.
- 7.4.2** Requests for approval for Overt Engagement of social media must describe the authorized mission, the CBP employees contractors, and persons using CBP systems in furtherance of the CBP mission authorized to use social media, the nexus to their assigned duties, the social media and any log-in credentials and profile information (including names, email addresses, photographs, etc.) used, and the authority to conduct the program.
- 7.4.3** Approved employees, contractors, and persons using CBP systems in furtherance of the CBP mission must identify themselves as associated with CBP by applying appropriate branding and disclaimers to distinguish the agency's activities from those of nongovernment actors. For example, Business Owners or Project Managers should add the CBP seal or emblem to the program's profile page on a social media website to indicate that it is an official agency presence.

7.5 Masked Monitoring

- 7.5.1** (b) (7)(E)



7.5.2 Approval of Masked Monitoring of social media must be re-approved every (b) (7) (E) [REDACTED]

7.5.3 (b) (7)(E) [REDACTED]

7.5.4 Requests for Approval for Masked Monitoring of social media must describe the authorized purpose for an operational need, the CBP employees, contractors, and persons using CBP systems in furtherance of the CBP mission authorized to conduct the Masked Monitoring of social media, the nexus to their assigned duties, the social media sites to be accessed, log-in credentials and profile information (including names, email addresses, photographs, etc.) used, and the authority to conduct the program. (b) (7)(E) [REDACTED]

7.5.5 Approved employees, contractors, and persons using CBP systems in furtherance of the CBP mission must comply with the specific terms for “Undercover Operational Use of Social Media and the Public Internet” as set forth in the attached CBP Operational Use of Social Media Rules of Behavior.

7.6 Undercover Engagement of Social Media

7.6.1 CBP employees, contractors, and persons using CBP systems in furtherance of the CBP mission may obtain approval to use social media for Undercover Engagement only when necessary for authorized law enforcement purposes with a clear nexus to their assigned duties and in conformance with existing undercover operations policies.

7.6.2 (b) (7)(E) [REDACTED]

7.6.3 (b) (7)(E) [REDACTED]

7.6.4 Approval of Undercover Engagement of Social Media must be re-approved every (b) (7)(E) through the procedures in 7.6.2.

7.6.5 Requests for Approval for Undercover Engagement of Social Media must describe the authorized purpose for an operational need, the CBP employees, contractors, and to persons using CBP systems in furtherance of the CBP mission authorized to use social media under cover, the social media sites used, log-in credentials and profile information (including names, email addresses, photographs, etc.) used, and the authority to conduct the program. (b) (7)(E) [REDACTED]

FOUO

(b) (7)(E)

- 7.6.6 Approved employees, contractors, and to persons using CBP systems in furtherance of the CBP mission must comply with the specific terms for “Under cover Operational Use of Social Media and the Public Internet” as set forth in the attached CBP Operational Use of Social Media Rules of Behavior.

8 PRIVACY INCIDENT HANDLING

- 8.1 Unauthorized use of social media will be considered a Privacy Incident.
- 8.2 In accordance with the DHS Privacy Incident Handling Guidance, all Privacy Incidents are to be immediately reported, as appropriate, to the DHS Security Operations Center (SOC) or CBP Computer Security Incident and Response Center (CSIRC) for review, investigation, mitigation, and remediation, as necessary.
- 8.3 Pursuant to CBP Delegation Order 11-001 “Delegation of Authority for Discipline and Adverse Actions” (April 6, 2011), unauthorized use of social media may be grounds for appropriate disciplinary action, as determined by the employee’s supervisor.

9 MEASUREMENT/INSPECTION

- 9.1 CBP’s Office of Internal Affairs, Management Inspections Division, shall develop and periodically, or at a minimum once each calendar year, administer an inspection mechanism to determine whether CBP Offices are in full compliance with this Directive.

10 DISCLOSURE

- 10.1 This Directive is for internal use only and may not be shared with the public.

11 NO PRIVATE RIGHT CREATED

This document is for internal CBP use only, and does not create or confer any rights, privileges, or benefits for any person or entity.



R. Gil Kerlikowske
Commissioner
U.S. Customs and Border Protection



**Homeland
Security**

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

Privacy Threshold Analysis
Version number: 01-2014
Page 1 of 12

PRIVACY THRESHOLD ANALYSIS (PTA)

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

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

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

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

PIA@hq.dhs.gov

Upon receipt from your component Privacy Office, the DHS Privacy Office will review this form. If a PIA is required, the DHS Privacy Office will send you a copy of the Official Privacy Impact Assessment Guide and accompanying Template to complete and return.

A copy of the Guide and Template is available on the DHS Privacy Office website, www.dhs.gov/privacy, on DHS Connect and directly from the DHS Privacy Office via email: pia@hq.dhs.gov, phone: 202-343-1717.



Homeland Security

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

Privacy Threshold Analysis
Version number: 01-2014
Page 2 of 12

PRIVACY THRESHOLD ANALYSIS (PTA)

SUMMARY INFORMATION

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

PROJECT OR PROGRAM MANAGER

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

INFORMATION SYSTEM SECURITY OFFICER (ISSO) (IF APPLICABLE)

| | | | |
|---------------|---------------------------|---------------|---------------------------|
| Name: | Click here to enter text. | | |
| Phone: | Click here to enter text. | Email: | Click here to enter text. |

Specific PTA Questions

| |
|--|
| 1. Reason for submitting the PTA: New PTA |
|--|



Homeland Security

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

Privacy Threshold Analysis
Version number: 01-2014

Page 3 of 12

This PTA provides an overview of CBP's (b) (7)(E) is a collaborative effort between CBP's Office of Intelligence (OI) and the Office of Professional Responsibility (OPR) to identify (b) (7)(E) to CBP personnel. (b) (7)(E)

(b) (7)(E)

OI's (b) (7)(E) through the collection of open source information and collaboration with other law enforcement and government partners, is designed to (b) (7)(E)

(b) (7)(E)

Partners include, but are not limited to the United States Marshal Service, other Department of Homeland Security components, The Federal Bureau of Investigation, State and Local Law Enforcement, the Intelligence Community and the Interagency. In order to (b) (7)(E) require the collection of Personally Identifiable Information (PII). The collection of PII will be limited to individuals (b) (7)(E)

(b) (7)(E) will collect PII through social media posts made in public forums, reports from concerned citizens, media reporting, and may receive (b) (7)(E)

(b) (7)(E) . Information acquired will be evaluated by CBP personnel (b) (7)(E)

(b) (7)(E)

No PII, including but not limited to screennames, social media handles, and IP address will be retained unless it is in support of (b) (7)(E) Under this effort, CBP elements supporting (b) (7)(E) will provide the information to both OPR, and OI, who will coordinate its upload into the (b) (7)(E)

(b) (7)(E) CBP necessarily collects information on individuals who, upon further investigation, do (b) (7)(E) to CBP employees or assets. In such cases, (b) (7)(E) will take no further action, but may continue to retain the information as necessary (b) (7)(E)

Additionally, (b) (7)(E) will not report on First Amendment protected speech or activities, however, if such activities (b) (7)(E) a report will be generated and sent to the (b) (7)(E) All personnel supporting this effort are trained law enforcement officers/agents, intelligence specialist and are familiar with the protections afforded under the law and the 1st Amendment. (b) (5)



Homeland Security

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

Privacy Threshold Analysis
Version number: 01-2014
 Page 4 of 12

(b) (5) [REDACTED] (b) (7)(E) will be augmented with personnel specifically trained to access, use, and protect PII when accessing social media. (b) (7)(E) personnel will respect privacy settings on all platforms, and will only access publicly available information.

| | |
|---|--|
| <p>2. Does this system employ any of the following technologies: <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> | <p><input type="checkbox"/> Closed Circuit Television (CCTV)</p> <p><input checked="" type="checkbox"/> Social Media</p> <p><input type="checkbox"/> Web portal¹ (e.g., SharePoint)</p> <p><input type="checkbox"/> Contact Lists</p> <p><input type="checkbox"/> None of these</p> |
|---|--|

| | |
|---|---|
| <p>3. From whom does the Project or Program collect, maintain, use, or disseminate information? <i>Please check all that apply.</i></p> | <p><input type="checkbox"/> This program does not collect any personally identifiable information²</p> <p><input checked="" type="checkbox"/> Members of the public</p> <p><input checked="" type="checkbox"/> DHS employees/contractors (list components):</p> <p><input type="checkbox"/> Contractors working on behalf of DHS</p> <p><input type="checkbox"/> Employees of other federal agencies</p> |
|---|---|

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

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.



Homeland Security

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

Privacy Threshold Analysis
Version number: 01-2014

Page 5 of 12

| | |
|----|------------|
| c. | (b) (7)(E) |
| d. | |
| e. | |

| | |
|--|---|
| <p>4(a) Does the project, program, or system retrieve information by personal identifier?</p> | <p><input type="checkbox"/> No. Please continue to next question. <input checked="" type="checkbox"/> Yes. If yes, please list all personal identifiers used: include but not limited to:</p> <div style="background-color: black; color: white; text-align: center; padding: 5px; font-size: 24px; font-weight: bold;">(b) (7)(E)</div> |
|--|---|



Homeland Security

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

Privacy Threshold Analysis
Version number: 01-2014
Page 6 of 12

| | |
|--|--|
| | (b) (7)(E) |
| <p>4(b) Does the project, program, or system use Social Security Numbers (SSN)?</p> | <p><input type="checkbox"/> No. <input checked="" type="checkbox"/> Yes. Entered as a case file within (b)(7)(E) or received as part of existing partner agency case file</p> |
| <p>4(c) If yes, please provide the specific legal basis and purpose for the collection of SSNs:</p> | <p>Collection will be used for identity verification as part of a CBP (b)(7)(E) or received as part of a partner agency case file. Authorities are outlined in CBP Directive No. 5410-003; CBP Directive 1440-027 Security Liaison Program; Participation under CBP Directive 4220-003A- Program for Fugitives wanted by U.S Customs; Title 18, Section 111, Assaulting, Resisting, or Impeding Certain Officers or Employees, and Section 1114, Protection of Officers and Employees of the United States; Executive Order 9397..</p> |
| <p>4(d) If yes, please describe the uses of the SSNs within the project, program, or system:</p> | <p>Identity verification.</p> |
| <p>4(e) If this project, program, or system is an information technology/system, does it relate solely to infrastructure?</p> | <p><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.</p> |



Homeland Security

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

Privacy Threshold Analysis
Version number: 01-2014

Page 7 of 12

| | |
|--|--|
| <p><i>For example, is the system a Local Area Network (LAN) or Wide Area Network (WAN)?</i></p> | |
| <p>4(f) If header or payload data³ is stored in the communication traffic log, please detail the data elements stored.</p> | |
| <p>Click here to enter text.</p> | |

| | |
|---|---|
| <p>5. Does this project, program, or system connect, receive, or share PII with any other DHS programs or systems⁴?</p> | <p><input type="checkbox"/> No.</p> <p><input checked="" type="checkbox"/> Yes. If yes, please list: (b) (7)(E) (b) (7)(E)</p> |
| <p>6. Does this project, program, or system connect, receive, or share PII with any external (non-DHS) partners or systems?</p> | <p><input type="checkbox"/> No.</p> <p><input checked="" type="checkbox"/> Yes. If yes, please list: Federal, State, Local Government & Law Enforcement Agencies. Foreign Government Law Enforcement Partners (b) (7)(E) comes from outside of the Continental United States.</p> |
| <p>6(a) Is this external sharing pursuant to new or existing information sharing access agreement (MOU, MOA, LOI, etc.)?</p> | <p>Existing</p> <p>Please describe applicable information sharing governance in place: For sharing information outside of DHS, (b) (7)(E) will follow CBP's process for sharing information (written request for authorization submitted to the CBP Privacy Office, followed by the submission of the DHS Form 191 to Privacy after the information has been released). In exigent circumstances</p> |

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.



Homeland Security

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

Privacy Threshold Analysis
Version number: 01-2014

Page 8 of 12

| | |
|--|--|
| | <p>(b) (7)(E) may pass the information prior to coordinating with CBP Privacy, but will follow up no later than the next business day. (b) (7)(E) may enter into Information Sharing Agreements or Memorandums of Understanding with Federal Partners. These agreements will follow OI Staffing requirements and will involve OI Policy, CBP's Office of Chief Counsel and CBP Privacy.</p> |
| <p>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?</p> | <p><input type="checkbox"/> No. <input checked="" type="checkbox"/> Yes. If yes, please list: (b) (7)(E) may assist with access to social media information and provide specific training related to access, use, and protection of PII.</p> |
| <p>8. Per NIST SP 800-53 Rev. 4, Appendix J, does the project, program, or system maintain an accounting of disclosures of PII to individuals who have requested access to their PII?</p> | <p><input type="checkbox"/> No. What steps will be taken to develop and maintain the accounting: <input type="checkbox"/> Yes. In what format is the accounting maintained:</p> |
| <p>9. Is there a FIPS 199 determination?⁴</p> | <p><input checked="" type="checkbox"/> Unknown. <input type="checkbox"/> No. <input type="checkbox"/> Yes. Please indicate the determinations for each of the following:</p> <p>Confidentiality: <input type="checkbox"/> Low <input type="checkbox"/> Moderate <input type="checkbox"/> High <input type="checkbox"/> Undefined</p> <p>Integrity: <input type="checkbox"/> Low <input type="checkbox"/> Moderate <input type="checkbox"/> High <input type="checkbox"/> Undefined</p> |

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



Homeland Security

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

Privacy Threshold Analysis
Version number: 01-2014
Page 9 of 12

| | |
|--|---|
| | Availability: <input type="checkbox"/> Low <input type="checkbox"/> Moderate <input type="checkbox"/> High <input type="checkbox"/> Undefined |
|--|---|

PRIVACY THRESHOLD REVIEW

(TO BE COMPLETED BY COMPONENT PRIVACY OFFICE)

| | |
|--|---------------------|
| Component Privacy Office Reviewer: | (b) (6), (b) (7)(C) |
| Date submitted to Component Privacy Office: | May 29, 2018 |
| Date submitted to DHS Privacy Office: | June 13, 2018 |
| Component Privacy Office Recommendation: Please include recommendation below, including what new privacy compliance documentation is needed. | |
| (b) (5), (b) (7)(E) <div style="background-color: black; width: 100%; height: 100%; min-height: 300px;"></div> | |



Homeland Security

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

Privacy Threshold Analysis
Version number: 01-2014
Page 10 of 12

| |
|--|
| |
|--|

(TO BE COMPLETED BY THE DHS PRIVACY OFFICE)

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

DESIGNATION

| | |
|-------------------------------------|---|
| Privacy Sensitive System: | Yes If "no" PTA adjudication is complete. |
| Category of System: | IT System If "other" is selected, please describe: Click here to enter text. |
| Determination: | <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: | New PIA is required. If covered by existing PIA, please list: |
| SORN: | SORN coverage To Be Determined during the development of the PIA If covered by existing SORN, please list: DHS/CBP-024 Intelligence Records System (CIRS) System of Records, September 21, 2017, 82 FR 44198 |
| DHS Privacy Office Comments: | |



Homeland Security

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

Privacy Threshold Analysis
Version number: 01-2014
Page 11 of 12

Please describe rationale for privacy compliance determination above.

CBP Privacy is submitting this PTA because CBP's (b) (7)(E) is a collaborative effort between CBP's Office of Intelligence (OI) and the Office of Professional Responsibility (OPR) to identify

(b) (7)(E)

(b) (7)(E) will require the collection of PII that will be limited to individuals (b) (7)(E)
(b) (7)(E)

will collect PII through social media posts made in public forums, reports from concerned citizens, media reporting, and (b) (7)(E)

(b) (7)(E)

Information acquired will be evaluated by CBP personnel (b) (7)(E)

(b) (7)(E)

(b) (7)(E) No PII, including but not limited to screennames, social media handles, and IP address will be retained unless it is in support of the (b) (7)(E)

The DHS Privacy Office agrees that this initiative is privacy-sensitive, requiring PIA and SORN coverage. CBP Privacy is required to complete a New PIA to discuss the new information collection used to (b) (7)(E)

(b) (7)(E)

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

The DHS Privacy Office requires that a training be created for all individuals supporting the search and analysis of social media for CBP employees who are trained as Law Enforcement Officers/Agents, who access, use, and protect PII to determine what is and is not a 1st Amendment protected activity.



Homeland Security

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

Privacy Threshold Analysis

Version number: 01-2014

Page 12 of 12

CBP should understand the prohibitions surrounding collection of 1st Amendment-protected speech and activities, such as protest, pursuant to 5 U.S.C. § 552a(e)(7) requiring that agencies “maintain no record describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual about whom the record is maintained or unless pertinent to and within the scope of an authorized law enforcement activity.” During this use case, CBP will exercise the judicial “law enforcement activity” exception due to a) the limited nature in which (b) (7)(E) is collecting information in order to

(b) (7)(E)

(b) (7)(E) during the trial; and b) the limited timeframe of the potential collection (limited to the trial period only).

(b) (5)

This PTA will expire on September 2nd, 2018 due to the reliance of a PIA and potentially a SORN.



Homeland Security

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

Version date: July 24, 2012
Page 1 of 9

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

¹ Gathering 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](#).



Homeland Security

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

Version date: July 24, 2012
Page 2 of 9

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.



Homeland Security

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

Version date: July 24, 2012
Page 3 of 9

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:

Name of Component: Customs and Border Protection

Contact Information: (b) (6), (b) (7)(C) Director, (b) (7)(E) Office of Intelligence and Investigative Liaison (b) (6), (b) (7)(C)

Counsel² Contact Information: Marc Bennett Courey, Office of Chief Counsel, Enforcement Section

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

- **Automated Targeting System- Targeting Framework.**

Applicable Privacy Impact Assessment(s) (PIA):

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;”

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

[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.”

² Counsel 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 Border Encounter SMOUT include CBP Officers (CBPO) and Border Patrol Agents (BPA). This SMOUT encompasses (b) (7)(E) only, as defined in CBP Directive 5410-003, (b) (7)(E). After determining a traveler requires additional inspection, CBP Officers and Border Patrol Agents perform checks on biographic information provided by the traveler at or between Ports of Entry. CBP personnel who (b) (7)(E) may access and review information, at their discretion, to perform queries on travelers' biographic information as they are undergoing secondary examination at a Port of Entry or between the ports of entry. Information gained through these operations may only be used by CBP personnel consistent with the legal authority of CBP, including admissibility determinations and other decisions as part of the inspection process. Information gained via social media as revealed by (b) (7)(E) may be retained in records of examinations or case files in the Automated Targeting System's Targeting Framework (ATS-TF), if deemed necessary (b) (7)(E)

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]



Homeland Security

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

Version date: July 24, 2012
Page 5 of 9

CBP personnel may use mechanisms, such as the (b) (7)(E) (b) (7)(E) to access social media websites normally restricted from CBP workstations. (b) (7)(E)

(b) (7)(E) Information collected using social media is stored in the (b) (7)(E) (b) (7)(E)

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

Under section 235 of the Immigration and Nationality Act and its implementing regulations, CBP Officers and Border Patrol Agents have several enforcement authorities and responsibilities associated with inspections at a port of entry. 8 U.S.C. § 1225; see also 8 CFR 287.2 (stating that a special agent in charge, port director, or chief patrol agent shall initiate an investigation when he has reason to believe there has been a criminal immigration violation); 8 CFR 287.4 (stating that several positions within Border Patrol may issue subpoenas to be used in criminal or civil investigations); 8 CFR 287.9 (stating that Border Patrol agents must obtain a search warrant prior to conducting a search in a criminal investigation unless a specific exemption to the warrant requirement is authorized by statute or recognized by courts). See also 19 U.S.C. §§ 482, 1467, 1496, 1582, and 1589a, and 19 CFR Part 162.

(b) (5)

- 3. Is this use of social media in development or operational?
 In development. Operational. Date first launched:
Unknown
- 4. Please attach a copy of the Rules of Behavior that outline the requirements below.

Attached are the CBP Directive and Rules of Behavior.



Homeland Security

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

Version date: July 24, 2012

Page 6 of 9

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;

(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;

(b) (7)(E)

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

Yes. No. If not, please explain:

(b) (7)(E)

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;



Homeland Security

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

Version date: July 24, 2012
Page 7 of 9

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:

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:



Homeland Security

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

Version date: July 24, 2012
Page 8 of 9

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

DATE reviewed by the DHS Privacy Office: December 17, 2015

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

DESIGNATION

This program is covered by the following Privacy Impact Assessment and Privacy Act System of Records Notice:

PIA: DHS/CBP/PIA-006(b) Automated Targeting System (ATS) Update (June 1, 2012)

SORN: DHS/CBP-006 - Automated Targeting System May 22, 2012, 77 FR 30297

DHS Privacy Office Determination

Program has met requirements to use social media for the stated authorized operational purposes, and must continue compliance with the requirements above.

Program has not yet met requirements to utilize social media for operational purposes.

Program authorities do not authorize operational use of social media.

Rules of Behavior do not comply. <Please explain analysis.>

Training required.

Additional Privacy compliance documentation is required:

A PIA is required.

New.

Updated. <Please include the name and number of PIA to be updated here.>



Homeland Security

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

Version date: July 24, 2012

Page 9 of 9

A SORN is required:

New.

Updated. <Please include the name and number of SORN to be updated here.>

DHS PRIVACY OFFICE COMMENTS

The DHS Privacy office finds that CBP's use of social media for Border Encounter Research is consistent with existing privacy compliance documentation and the DHS MD 110-01 requirements.

CBP will conduct attributable, (b) (7)(E) only. CBP Officers and Border Patrol Agents (b) (7)(E)

CBP does not (b) (7)(E)
(b) (7)(E)

Any information collected from social media will be stored within the CBP Automated Targeting System (ATS), Targeting Framework (TF) module. Per the 2012 ATS PIA, (b) (7)(E)

[Redacted text block]



Homeland Security

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

Version date: July 24, 2012
Page 1 of 8

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.

¹ Gathering 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](#).



Homeland Security

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

Version date: July 24, 2012

Page 2 of 8

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:

Name of Component: Customs and Border Protection

Contact Information: (b) (6), (b) (7)(C) Director, (b) (7)(E) Office of Intelligence and Investigative Liaison (b) (6), (b) (7)(C)

Counsel² Contact Information: Marc Bennett Courey, Office of Chief Counsel, Enforcement Section

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

- Automated Targeting System- Targeting Framework.

Applicable Privacy Impact Assessment(s) (PIA):

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;”

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

[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.”

- Analytical Framework for Intelligence

DHS/CBP/PIA-010 – [Analytical Framework for Intelligence](#) (AFI), June 1, 2012. Per the AFI PIA § 2.1 Identify the information the project collects, uses, disseminates, or maintains: “... DHS AFI analysts may upload information that the user believes is relevant to a project, including information publicly available on the Internet.”

[DHS/CBP-017 – Analytical Framework for Intelligence System](#) June 7, 2012 77 FR 13813. Per the Record Source Categories: “Additionally, AFI permits analysts to upload and store any information from any source including public and commercial sources, which may be relevant to projects, responses to RFIs, or final intelligence products.”

² Counsel 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 include CBP Intelligence Research Specialists, CBP Officers, Border Patrol Agents, and Air & Marine personnel. This SMOUT encompasses both (b) (7)(E)

(b) (7)(E) CBP personnel who receive specific prior supervisory approval may

(b) (7)(E)

(b) (7)(E) Under this SMOUT, CBP

personnel may use mechanisms, (b) (7)(E)

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

Information

gained through these operations may only be used consistent with the legal authorities of CBP. For example, this may include (b) (7)(E)

(b) (7)(E)

(b) (7)(E) Any

information gained via social media as (b) (7)(E)

may be retained, (b) (7)(E)

in the Automated Targeting System's Targeting Framework (ATS-TF) or the Analytical Framework for Intelligence. (b) (7)(E)

(b) (7)(E)

(b) (7)(E)

. This information may be stored in AFI or ATS-TF.

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

Under 235 of the Immigration and Nationality Act and its implementing regulations CBP Officers and Border Patrol Agents have several enforcement authorities and responsibilities associated with inspections at a port of entry. 8 U.S.C. § 1225; see also 8 CFR 287.2 (stating that a special agent in charge, port



Homeland Security

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

Version date: July 24, 2012
Page 4 of 8

director, or chief patrol agent shall initiate an investigation when he has reason to believe there has been a criminal immigration violation); 8 CFR 287.4 (stating that several positions within Border Patrol may issue subpoenas to be used in criminal or civil investigations); 8 CFR 287.9 (stating that Border Patrol agents must obtain a search warrant prior to conducting a search in a criminal investigation unless a specific exemption to the warrant requirement is authorized by statute or recognized by courts). *See also* 19 U.S.C. § 482, 1467, 1496, 1582, and 1589a, and 19 CFR Part 162.

(b) (5)

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

In development. Operational. Date first launched: Unknown

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

Attached are the CBP Directive and Rules of Behavior.

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;

(b) (7)(E)



Homeland Security

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

Version date: July 24, 2012
Page 5 of 8

- c) *Public interaction.* Access publicly available information through social media only by reviewing posted information without interacting with any individual who posted the information;

(b) (7)(E)



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

(b) (7)(E)



- 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:



Homeland Security

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

Version date: July 24, 2012
Page 6 of 8

- 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:

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:



Homeland Security

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

Version date: July 24, 2012
Page 7 of 8

DHS SOCIAL MEDIA DOCUMENTATION

(To be Completed by the DHS Privacy Office)

DATE reviewed by the DHS Privacy Office: May 13, 2015

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

DESIGNATION

This program is covered by the following Privacy Impact Assessment and Privacy Act System of Records Notice:

PIA: DHS/CBP/PIA-006 ATS

SORN: DHS/CBP-006 ATS

DHS Privacy Office Determination

Program has met requirements to use social media for the stated authorized operational purposes, and must continue compliance with the requirements above.

Program has not yet met requirements to utilize social media for operational purposes.

Program authorities do not authorize operational use of social media.

Rules of Behavior do not comply. <Please explain analysis.>

Training required.

Additional Privacy compliance documentation is required:

A PIA is required.

New.

Updated. <Please include the name and number of PIA to be updated here.>

A SORN is required:

New.

Updated. <Please include the name and number of SORN to be updated here.>



**Homeland
Security**

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

Version date: July 24, 2012
Page 8 of 8

DHS PRIVACY OFFICE COMMENTS

CBP's use of social media for Operational Awareness is compliant with the DHS social media directive MD 110-01-011.

This SMOUT is intended to address (b) (7)(E). The ATS PIA referenced references CBP's use of information on the internet. The CBP Directive on the Operational Use of Social Media, CBP defines (b) (7)(E) as follows:

- (b) (7)(E)

- (b) (7)(E)

(b) (7)(E)



Homeland Security

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

DHS OPERATIONAL USE OF SOCIAL MEDIA

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

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

Communications and outreach with the public authorized by the Office of Public Affairs (covered by the existing PIAs: [DHS/ALL/PIA-031 - Use of Social Networking Interactions and Applications Communications/Outreach/Public Dialogue](#) and [DHS/ALL/PIA-036 - Use of Unidirectional Social Media Applications](#));

The conduct of authorized intelligence activities carried out by the Office of Intelligence and Analysis, the intelligence and counterintelligence elements of the United States Coast Guard, or any other Component performing authorized foreign intelligence or counterintelligence functions, in accordance with the provisions of Executive Order 12333, as amended.

This template shall be used to document the process to be followed by all programs engaging in operational uses of social media; to identify information technology systems, technologies, rulemakings, programs, or pilot projects that involve PII and other activities that otherwise impact the privacy of individuals as determined by the Chief Privacy Officer; and to assess whether there is a need for additional Privacy Compliance Documentation. Components may appeal to the Deputy Secretary for Homeland Security if there is disagreement over the DHS Privacy Office determination of privacy compliance for the operational use of social media.



Homeland Security

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

DHS OPERATIONAL USE OF SOCIAL MEDIA

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

Summary Information

Name of SMOUT: Border Patrol Intelligence – (b) (7)(E)

Date submitted for review: November 23, 2015

Name of Component: U.S. Customs and Border Protection

Contact Information: Assistant Chief (b) (6), (b) (7)(C) United States Border Patrol.
(b) (6), (b) (7)(C) @cCBP.DHS.GOV, (b) (6), (b) (7)(C)

Counsel Contact Information: Marc Bennett Courey, Office of Chief Counsel, Enforcement

IT System(s) where social media data is stored: Automated Targeting System-Targeting Framework and the Analytical Framework for Intelligence (if included in a finished intelligence product)

Applicable Privacy Impact Assessment(s) (PIA):

- DHS/CBP/PIA-006(e) [Automated Targeting System \(ATS\) Update](#), January 13, 2017. Per the ATS PIA, ATS maintains the official record “for certain law enforcement and/or intelligence data, reports, and projects developed by CBP analysts that may include public source information;”
- DHS/CBP/PIA-010a – [Analytical Framework for Intelligence](#) (AFI), September 1, 2016. Per the AFI PIA § 2.1 Identify the information the project collects, uses, disseminates, or maintains: “... DHS AFI analysts may upload information that the user believes is relevant to a project, including information publicly available on the Internet.”

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

Raw intelligence collected by CBP is covered by: DHS/CBP-024 Intelligence Records System (CIRS), September 21, 2017 82 FR 44198. This system of records allows CBP to collect and consolidate information from multiple sources, including law enforcement agencies and agencies of the U.S. Intelligence Community, in order to enhance CBP’s ability to: Identify, apprehend, or prosecute individuals who pose a potential law enforcement or security risk; aid in the enforcement of the customs and immigration laws, and other laws enforced by DHS at the border; and enhance U.S. border security.

Records maintained within the CIRS system of records include information collected by CBP for an intelligence purpose that is not covered by an existing DHS SORN and finished intelligence products. This information may include:



Homeland Security

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

- Biographic information (name, date of birth, Social Security number, alien registration number, citizenship/immigration status, passport information, addresses, phone numbers, etc.);
- Records of immigration enforcement activities or law enforcement investigations/activities;
- Information (including documents and electronic data) collected by CBP from or about individuals during investigative activities and border searches;
- Records of immigration enforcement activities and law enforcement investigations/activities that have a possible nexus to CBP's law enforcement and immigration enforcement responsibilities or homeland security in general;
- Law enforcement, intelligence, crime, and incident reports (including financial reports under the Bank Secrecy Act and law enforcement bulletins) produced by DHS and other government agencies;
- U.S. visa, border, immigration, and naturalization benefit data, including arrival and departure data;
- Terrorist watchlist information and other terrorism-related information regarding threats, activities, and incidents;
- Lost and stolen passport data;
- Records pertaining to known or suspected terrorists, terrorist incidents, activities, groups, and threats;
- CBP-generated intelligence requirements, analysis, reporting, and briefings;
- Information from investigative and intelligence reports prepared by law enforcement agencies and agencies of the U.S. foreign intelligence community;
- **Articles, public-source data (including information from social media), and other published information on individuals and events of interest to CBP;**
- Audio and video records retained in support of CBP's law enforcement, national security, or other homeland security missions;
- Records and information from government data systems or retrieved from commercial data providers in the course of intelligence research, analysis, and reporting;
- Reports of suspicious activities, threats, or other incidents generated by CBP or third parties;
- Additional information about confidential sources or informants; and
- Metadata, which may include but is not limited to transaction date, time, location, and frequency.

Finished Intelligence Products produced by CBP are covered by: DHS/CBP-017 – Analytical Framework for Intelligence System, June 7, 2012 77 FR 13813. The purpose of this system is to enhance DHS's ability to: Identify, apprehend, and/or prosecute individuals who pose a potential law enforcement or security



Homeland Security

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

risk; aid in the enforcement of the customs and immigration laws, and other laws enforced by DHS at the border; and enhance United States security. AFI uses data to:

- (1) Identify individuals, associations, or relationships that may pose a potential law enforcement or security risk, target cargo that may present a threat, and assist intelligence product users in the field in preventing the illegal entry of people and goods, or identifying other violations of law;
- (2) Allow analysts to conduct additional research on persons and/or cargo to understand whether there are patterns or trends that could identify potential law enforcement or security risks; and
- (3) Allow finished intelligence product users with a need to know to query or receive relevant finished intelligence products.



DHS OPERATIONAL USE OF SOCIAL MEDIA SPECIFIC QUESTIONS

1. Describe the category of use for collecting personally identifiable information from social media sources. Examples include: law enforcement intelligence, criminal investigations, background investigations, administrative investigations, professional responsibility investigations, benefit or employment determinations, or situational awareness. If use does not fit into one of these categories, please describe in full below. If your component has multiple categories of use, please submit separate template for each category.

CBP is submitting this SMOUT to request access to social media for (b) (7)(E) as defined by the CBP Operational Use of Social Media Policy¹ for Border Patrol agents assigned to the Border Patrol Sector Intelligence Units (SIU), and the USBP Headquarters Intelligence Division (Border Patrol Intelligence Agents (BPA-Is), Supervisory Border Intelligence Agents (SBPA-Is) or Border Patrol Intelligence Enterprise (BPIE) intelligence analysts). The Sector Intelligence Unit (SIU) operates primarily at the tactical level, working in coordination with the HQ Intelligence Division, sector command staff and stations. The four primary functions of the SIU are to collect information that provides current intelligence, conduct targeted enforcement operations, provide analysis, and provide support to ongoing intelligence operations. This allows the SIU to produce sector level intelligence products for wider consumption, including federal, state, local, and tribal stakeholders.

The SIU will support sector command staff and respond to intelligence collection requirements both at the sector and national level. The SIU strives for integration with all stations within their respective sectors by working with station staff and collateral intelligence agents to address the station commander's objectives, gather information, and produce intelligence products for local and national consumption. In addition, SIU agents assigned to Border Patrol stations will act as subject matter experts to educate station personnel as to their role within the BPIE. The SIU has the following responsibilities:

- Understand intelligence priorities
- Produce quality, finished, information and intelligence products
- Ensure constant flow of information and intelligence
- Protect and promote intelligence integrity and objectivity
- Integrate intelligence into operational activities to reduce uncertainty
- Drive sector and station operations with collections and analytical support
- Understand and operate within intelligence doctrine, capabilities and limitations

¹ CBP Directive 5410-003 (January 2, 2015) defines

(b) (7)(E)

(b) (7)(E)



Homeland Security

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

- Receive and incorporate feedback from agents, station staff and sector management

The primary mission of the SIU is to gather and synthesize information. To do so, Border Patrol agents who are assigned to the SIU or Headquarters Intelligence Division undergo specific training for the intelligence enterprise. All SIU personnel are trained and certified to perform the intelligence collection, management, and analytical functions necessary for their respective roles. Individuals responsible for providing that information must have the necessary skills and competencies necessary to provide that intelligence.

To accomplish their intelligence functions, these specialized USBP intelligence personnel must use (b) (7)(E)

(b) (7)(E)

General Procedures

Consistent with the CBP Operational Use of Social Media Policy,² once this SMOUT has been approved by the DHS Privacy Office, there are additional procedural requirements for (b) (7)(E)

(b) (7)(E) Border Patrol agents who are assigned to Sector Intelligence Units or the USBP Headquarters Intelligence Division must obtain approval to use social media for (b) (7)(E) only when necessary for authorized law enforcement purposes with a clear nexus to their assigned duties and in conformance with existing (b) (7)(E)

(b) (7)(E)

Individual Access Requests

Border Patrol agents who are assigned to (b) (7)(E)

(b) (7)(E)

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

(b) (7)(E)



Homeland Security

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

(b) (7)(E)

Upon approval of this template and in accordance with the individual access procedures outlined in CBP Directive 5410-003, USBP intelligence personnel may use the (b) (7)(E)

(b) (7)(E)

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

6 U.S.C. § 211(e) establishes the Border Patrol in CBP and sets forth certain statutory duties, including the responsibility to: “(A) serve as the law enforcement office of U.S. Customs and Border Protection with primary responsibility for interdicting persons attempting to illegally enter or exit the United States or goods being illegally imported into or exported from the United States at a place other than a designated port of entry; (B) deter and prevent the illegal entry of terrorists, terrorist weapons, persons, and contraband; and (C) carry out other duties and powers prescribed by the Commissioner.”

Under section 287(b) of the Immigration and Nationality Act (INA) (8 U.S.C. § 1357(b)), authorized Border Patrol agents “have the power and authority . . . to take and consider evidence concerning the privilege of any person to enter, reenter, pass through, or reside in the United States, or concerning any matter which is material or relevant to the enforcement of [the INA] . . .” See also 8 CFR 287.2 (stating that a special agent in charge, port director, or chief patrol agent shall initiate an investigation when he has reason to believe there has been a criminal immigration violation). Additionally, 19 U.S.C. § 1589a provides enforcement authority to customs officers, including Border Patrol agents.

(b) (7)(E)

(b) (5)

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

In development. Operational. Date first launched:

USBP use of social media for (b) (7)(E) is pending the approval of this SMOUT.

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

Attached are the CBP Directive and Rules of Behavior.

6. Please describe the Rules of Behavior in effect for the listed operational use of social media. If users do NOT follow a particular Rule, please detail reasoning for not following that Rule:



Homeland Security

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

Equipment. Use only government-issued equipment when engaging in the operational use of social media;

Yes. No. If not, please explain:

Email and accounts. Use online screen names or identities that indicate an official DHS affiliation and use DHS email addresses to open accounts used when engaging in social media in the performance of their duties;

(b) (7)(E)

(b) (7)(E)

Public interaction. Access publicly available information through social media only by reviewing posted information without interacting with any individual who posted the information;

(b) (7)(E)

(b) (7)(E)

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

(b) (7)(E)

(b) (7)(E)

PII collection: Collect the minimum PII necessary for the proper performance of their authorized duties except for systems subject to Final Rules for Exemption from certain aspects of the Privacy Act;

Yes. No. If not, please explain:

PII safeguards. Protect PII as required by the Privacy Act (if applicable) and DHS privacy policy;

Yes. No. If not, please explain:

Documentation. Document operational use of social media, including date, site(s) accessed, information collected and how it was used.

Yes. No. If not, please explain:

Training. Users complete annual privacy training which has been approved by Component Privacy Officer (or Privacy Point of Contact) based upon training materials provided by the DHS Privacy Office.



Homeland Security

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

Training must include, at minimum: legal authorities, acceptable operational uses of social media, access requirements, and requirements for documenting operational uses of social media.

Yes. No. If not, please explain:

Yes, employees self-certify that they have read and understood their Component Rules of Behavior.

Yes, Component Privacy Officers or PPOCs maintain a record of employee attendance at privacy training that includes training on the Rules of Behavior.

No. If not, please explain:



Homeland Security

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

DHS SOCIAL MEDIA DOCUMENTATION

(To be completed by the DHS Privacy Office)

DATE reviewed by the DHS Privacy Office: 11/27/2017

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

DESIGNATION

This program is covered by the following Privacy Impact Assessment and Privacy Act System of Records Notice:

PIA:

DHS/CBP/PIA-006 Automated Targeting System (ATS)

DHS/CBP/PIA-010 Analytical Framework for Intelligence (AFI)

SORN:

DHS/CBP-017 Analytical Framework for Intelligence System, June 7, 2012 77 FR 13813

DHS/CBP-024 Intelligence Records System (CIRS) System of Records, September 21, 2017, 82 FR 44198

- 1. (b) (7)(E) [Redacted]

(b) (5) [Redacted]

3. Rules of Behavior Content: (Check all items that apply.)



Homeland Security

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

a. *Equipment.*

Users must use government-issued equipment. (b) (7)(E)
(b) (7)(E)

Users must use government-issued equipment. (b) (7)(E)
(b) (7)(E)

b. *Email and accounts.*

(b) (7)(E)

c. *Public interaction.*

(b) (7)(E)

d. *Privacy settings.*

Users may disregard privacy settings.

Users must respect individual privacy settings. (b) (7)(E)

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

e. *PII storage:*

PII is maintained in an exempted Privacy Act System of Records.

Please list applicable SORN here: DHS/CBP-017 Analytical Framework for Intelligence (AFI) System
DHS/CBP-024 Intelligence Records System (CIRS)

PII is maintained in a Privacy Act Systems of Records.

Please list applicable SORN here:

f. *PII safeguards.*

PII is protected as required by the Privacy Act and DHS privacy policy.

Only a minimal amount of PII is collected and safeguarded, consistent with



Homeland Security

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

g. *Documentation.*

- Users must appropriately document their use of social media, and collection of information from social media website.
- Documentation is not expressly required.

h. *Training.*

- All users must complete annual privacy training that has been approved by Component Privacy Officer. Training includes:
 - Legal authorities;
 - Acceptable operational uses of social media;
 - Access requirements;
 - Applicable Rules of Behavior; and
 - Requirements for documenting operational uses of social media.
- Mechanisms are (or will be) in place to verify that users have completed training.
 - Yes, employees self-certify that they have read and understood their Component Rules of Behavior.
 - Yes, Component Privacy Officers or PPOCs maintain a record of employee attendance at privacy training that includes training on the Rules of Behavior.
 - No, certification of training completion cannot be verified.

DHS Privacy Office Determination

- Program has met requirements to use social media for the stated authorized operational purposes, and must continue compliance with the requirements above.
- Program has not yet met requirements to utilize social media for operational purposes.
 - Program authorities do not authorize operational use of social media.
 - Rules of Behavior do not comply. <Please explain analysis.>
 - Training required.

Additional Privacy compliance documentation is required:



Homeland Security

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

- A PIA is required.
 - New.
 - Updated. <Please include the name and number of PIA to be updated here.>
- A SORN is required:
 - New.
 - Updated. <Please include the name and number of SORN to be updated here.>

DHS PRIVACY OFFICE COMMENTS

CBP is submitting this SMOUT to discuss the request for access to social media for (b) (7)(E) as defined by the CBP Operational Use of Social Media Policy for U.S. Border Patrol (USBP) agents assigned to the Border Patrol Sector Intelligence Units (SIU), and the USBP Headquarters Intelligence Division. The primary mission of the SIU is to gather and synthesize information. (b) (7)(E)

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Border Patrol agents who are assigned to SIU or the USBP Headquarters Intelligence Division (b) (7)(E)

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] Any information collected from social media will be stored within the Automated Targeting System-Targeting Framework (ATS-TF) and the Analytical Framework for Intelligence (AFI) (if included in a finished intelligence product). Per the ATS PIA, ATS-TF allows authorized users to attach public source information, such as responsive Internet links and related documents, to an assigned report and/or project and search for any text contained within the system via full text search functionality. Per the AFI PIA, analysts may upload information that the user believes is relevant to a project, including information publicly available on the Internet.

SORN coverage for raw intelligence collected by CBP is covered by DHS/CBP-024 Intelligence Records System (CIRS), which covers the collection and consolidation of information from multiple sources, including law enforcement agencies and agencies of the U.S. Intelligence Community, in order to enhance CBP's ability to: identify, apprehend, or prosecute individuals who pose a potential law enforcement or



Homeland Security

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

security risk; aid in the enforcement of the customs and immigration laws, and other laws enforced by DHS at the border; and enhance U.S. border security. Records maintained within the CIRS may include “articles, public-source data (including information from social media), and other published information on individuals and events of interest to CBP.” SORN coverage for finished intelligence products produced by CBP is provided by DHS/CBP-017 Analytical Framework for Intelligence System, which covers the collection of information to enhance DHS’s ability to: identify, apprehend, and/or prosecute individuals who pose a potential law enforcement or security risk; aid in the enforcement of the customs and immigration laws, and other laws enforced by DHS at the border; and enhance U.S. security.

ORDER FOR SUPPLIES OR SERVICES

PAGE OF PAGES

1 8

IMPORTANT: Mark all packages and papers with contract and/or order numbers.

| | | | | | |
|--|--|---|----------------------|--|--|
| 1. DATE OF ORDER 9/20/2018 | | 2. CONTRACT NO. (if any) HSHQDC-12-D-00013 | | 6. SHIP TO: | |
| 3. ORDER NO. 70B04C18F00001093 | | 4. REQUISITION/REFERENCE NO. 0020099198 | | a. NAME OF CONSIGNEE See Attached Delivery Schedule | |
| 5. ISSUING OFFICE (Address correspondence to) DHS - Customs & Border Protection Customs and Border Protection 1300 Pennsylvania Ave, NW Procurement Directorate - NP 1310 Washington DC 20229 | | | | b. STREET ADDRESS | |
| c. CITY | | d. STATE | e. ZIP CODE | | |
| 7. TO: | | | | f. SHIP VIA | |
| a. NAME OF CONTRACTOR PANAMERICA COMPUTERS, INC. | | | | 8. TYPE OF ORDER | |
| b. COMPANY NAME | | | | <input type="checkbox"/> a. PURCHASE -- Reference Your BID # 565079305. Please furnish the following on the terms and conditions specified on both sides of this order and on the attached sheet, if any, including delivery as indicated. | |
| c. STREET ADDRESS 1386 BIG OAK RD. | | | | <input checked="" type="checkbox"/> b. DELIVERY -- Except for billing instructions on the reverse, this delivery order is subject to instructions contained on this side only of this form and is issued subject to the terms and conditions of the above-numbered contract. | |
| d. CITY LURAY | | e. STATE VA | f. ZIP CODE 22835 | | |
| 9. ACCOUNTING AND APPROPRIATION DATA | | | | 10. REQUISITIONING OFFICE (b) (6), (b) (7)(C) | |

| | | | | | |
|--|---|--|---|--|------------------|
| 11. BUSINESS CLASSIFICATION (Check appropriate box(es)) | | | | | 12. F.O.B. POINT |
| <input checked="" type="checkbox"/> a. SMALL | <input type="checkbox"/> b. OTHER THAN SMALL | <input type="checkbox"/> c. DISADVANTAGED | <input type="checkbox"/> d. WOMEN-OWNED | <input checked="" type="checkbox"/> e. HUBZone | Not applicable |
| <input type="checkbox"/> f. SERVICE-DISABLED VETERAN-OWNED | <input type="checkbox"/> g. WOMEN-OWNED SMALL BUSINESS (WOSB) ELIGIBLE UNDER THE WOSB PROGRAM | <input type="checkbox"/> h. ECONOMICALLY DISADVANTAGED WOMEN-OWNED SMALL BUSINESS (EDWOSB) | | | |

| | | | | |
|---------------|---------------|------------------------|--|--|
| 13. PLACE OF | | 14. GOVERNMENT B/L NO. | 15. DELIVER TO F.O.B POINT ON OR BEFORE (Date) 09/21/2018 | 16. DISCOUNT TERMS Within 30 days Due net |
| a. INSPECTION | b. ACCEPTANCE | | | |

| 17. SCHEDULE (See reverse for Rejections) | | | | | | |
|---|--------------------------|----------------------|----------|----------------|------------|--------|
| ITEM NO. (a) | SUPPLIES OR SERVICES (b) | QUANTITY ORDERED (c) | UNIT (d) | UNIT PRICE (e) | AMOUNT (f) | Accept |
| 10 | (b) (7)(E) | 1.000 | EA | (b) (4) | | |

| | | | | | | |
|--|--|---------------------------|----------------------|-----------------|--|-------------------------|
| 18. SHIPPING POINT | | 19. GROSS SHIPPING WEIGHT | | 20. INVOICE NO. | | 17(h)TOT. (Cont. pages) |
| 21. MAIL INVOICE TO: | | | | | | |
| a. NAME DHS - Customs & Border Protection | | Commercial Accounts Sect. | | | | \$0.00 |
| b. STREET ADDRESS (or P.O. Box) 6650 Telecom Drive, Suite 100 | | | | | | |
| c. CITY Indianapolis | | d. STATE IN | e. ZIP CODE 46278 | | | \$2,206,058.25 |
| 17(i) GRAND TOTAL | | | | | | |

| | | | |
|--|--|--|--|
| 22. UNITED STATES OF AMERICA BY (Signature) (b) (6), (b) (7)(C) | | 23. NAME (Type) (b) (6), (b) (7)(C) | |
| TITLE: CONTRACTING/ORDERING OFFICER | | | |

AUTHORIZED FOR LOCAL REPRODUCTION
PREVIOUS EDITION NOT USABLE

| | | | |
|----------------------------|--|--------------------------------|----------------------|
| DATE OF ORDER 9/20/2018 | CONTRACT NO. (if any) HSHQDC-12-D-00013 | ORDER NO. 70B04C18F00001093 | PAGE OF PAGES 2 8 |
|----------------------------|--|--------------------------------|----------------------|

Federal Tax Exempt ID: (b) (3) (A)

Emailing Invoices to CBP. Do not mail or email invoices to CBP. Invoices must be submitted via the IPP website, as detailed under Electronic Invoicing and Payment Requirements in the attached terms and conditions.

NOTES:

This Firm Fixed Price delivery order, 70B04C18F00001093, is issued against the Department of Homeland Security FirstSource II Contract HSHQDC-12-D-00013 for (b) (7)(E) Licenses and Maintenance in support of (b) (7)(E) (b) (7)(E). The Statement of Work will be provided with the Award Distribution email.

Reference Bid # 565079305, dated 9/05/2018, from FedBid Buy #945260_01

The Period of Performance for 70B04C18F00001093 will be (b) (7)(E)

The Contracting Officer's Representative for this order is:

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

Address: (b) (7)(E)

(b) (7)(E)

Tel. #: (b) (6), (b) (7)(C)

Fax. #:

(b) (6), (b) (7)(C) @cbp.dhs.gov

Invoices shall be sent to:

IPP.gov in accordance with Section 10.5 of the SOW.

All Terms and Conditions of the FirstSource II Contract HSHQDC-12-D-00013 are in full force and effect.

70B04C18F00001093

**ITEMS AND PRICES, DELIVERY SCHEDULE AND ACCOUNTING DATA
FOR
DELIVERY ORDER: 70B04C18F00001093**

I.1 SCHEDULE OF SUPPLIES/SERVICES

| ITEM # | DESCRIPTION | QTY | UNIT | UNIT PRICE | EXT. PRICE |
|--------|-------------|-------|------|------------|------------|
| 10 | (b) (7)(E) | 1.000 | EA | (b) (4) | |

Total Funded Value of Award:

\$2,206,058.25

I.2 ACCOUNTING and APPROPRIATION DATA

| ITEM # | ACCOUNTING and APPROPRIATION DATA | AMOUNT |
|--------|--|----------------|
| 10 | 6100.315BUSCSGLCS0942715000Z00018500TT0600000000 IU549315B TAS# 07020182018 0530000 | \$2,206,058.25 |

I.3 DELIVERY SCHEDULE

| DELIVER TO: | ITEM # | QTY | DELIVERY DATE |
|---|--------|-------|---------------|
| Customs and Border Protection (b) (7)(E) | 10 | 1.000 | (b) (7)(E) |

I.4 52.232-39 UNENFORCEABILITY OF UNAUTHORIZED OBLIGATIONS (JUN 2013)

(a) Except as stated in paragraph (b) of this clause, when any supply or service acquired under this contract is subject to any End User License Agreement (EULA), Terms of Service (TOS), or similar legal instrument or agreement, that includes any clause requiring the Government to indemnify the Contractor or any person or entity for damages, costs, fees, or any other loss or liability that would create an Anti-Deficiency Act violation (31 U.S.C. 1341), the following shall govern:

(1) Any such clause is unenforceable against the Government.

(2) Neither the Government nor any Government authorized end user shall be deemed to have agreed to such clause by virtue of it appearing in the EULA, TOS, or similar legal instrument or agreement. If the EULA, TOS, or similar legal instrument or agreement is invoked through an "I agree" click box or other comparable mechanism (e.g., "click-wrap" or "browse-wrap" agreements), execution does not bind the Government or any Government authorized end user to such clause.

(3) Any such clause is deemed to be stricken from the EULA, TOS, or similar legal instrument or agreement.

(b) Paragraph (a) of this clause does not apply to indemnification by the Government that is expressly authorized by statute and specifically authorized under applicable agency regulations and procedures.

(End of clause)

I.5 52.232-40 PROVIDING ACCELERATED PAYMENTS TO SMALL BUSINESS SUBCONTRACTORS (DEC 2013)

(a) Upon receipt of accelerated payments from the Government, the Contractor shall make accelerated payments to its small business subcontractors under this contract, to the maximum extent practicable and prior to when such payment is otherwise required under the applicable contract or subcontract, after receipt of a proper invoice and all other required documentation from the small business subcontractor.

(b) The acceleration of payments under this clause does not provide any new rights under the Prompt Payment Act.

(c) Include the substance of this clause, including this paragraph (c), in all subcontracts with small business concerns, including subcontracts with small business concerns for the acquisition of commercial items.

70B04C18F00001093

(End of clause)

I.6 52.203-19 PROHIBITION ON REQUIRING CERTAIN INTERNAL CONFIDENTIALITY AGREEMENTS OR STATEMENTS (JAN 2017)

I.7 52.204-22 ALTERNATIVE LINE ITEM PROPOSAL (JAN 2017)

I.8 52.204-23 - PROHIBITION ON CONTRACTING FOR HARDWARE, SOFTWARE, AND SERVICES DEVELOPED OR PROVIDED BY KASPERSKY LAB AND OTHER COVERED ENTITIES (JUL 2018)

I.9 52.209-10 PROHIBITION ON CONTRACTING WITH INVERTED DOMESTIC CORPORATIONS (NOV 2015)

I.10 3052.205-70 ADVERTISEMENTS, PUBLICIZING AWARDS, AND RELEASES (SEP 2012) ALTERNATE I (SEP 2012)

- (a) The Contractor shall not refer to this contract in commercial advertising or similar promotions in such a manner as to state or imply that the product or service provided is endorsed or preferred by the Federal Government or is considered by the Government to be superior to other products or services.
- (b) All advertisements, releases, announcements, or other publication regarding this contract or the agency programs and projects covered under it, or the results or conclusions made pursuant to performance, must be approved by the Contracting Officer. Under no circumstances shall the Contractor, or anyone acting on behalf of the Contractor, refer to the supplies, services, or equipment furnished pursuant to the provisions of this contract in any publicity, release, or commercial advertising without first obtaining explicit written consent to do so from the Contracting Officer.

(End of clause)

I.11 52.224-3 PRIVACY TRAINING, ALTERNATE I (DEVIATION)

- (a) Definition. As used in this clause, personally identifiable information means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. (See Office of Management and Budget (OMB) *Circular A-130, Managing Federal Information as a Strategic Resource*).
- (b) The Contractor shall ensure that initial privacy training, and annual privacy training thereafter, is completed by contractor employees who--
 - (1) Have access to a system of records;
 - (2) Create, collect, use, process, store, maintain, disseminate, disclose, dispose, or otherwise handle personally identifiable information on behalf of an agency; or
 - (3) Design, develop, maintain, or operate a system of records (see also FAR subpart 24.1 and 39.105).
- (c) The contracting agency will provide initial privacy training, and annual privacy training thereafter, to Contractor employees for the duration of this contract. Contractor employees shall satisfy this requirement by completing *Privacy at DHS: Protecting Personal Information* accessible at <http://www.dhs.gov/dhs-security-and-training-requirements-contractors>. Training shall be completed within 30 days of contract award and be completed on an annual basis thereafter not later than October 31st of each year.
- (d) The Contractor shall maintain and, upon request, provide documentation of completion of privacy training to the Contracting Officer.
- (e) The Contractor shall not allow any employee access to a system of records, or permit any employee to create, collect, use, process, store, maintain, disseminate, disclose, dispose or otherwise handle personally identifiable information, or to design, develop, maintain, or operate a system of records unless the employee has completed privacy training, as required by this clause.
- (f) The substance of this clause, including this paragraph (f), shall be included in all subcontracts under this contract, when subcontractor employees will –

70B04C18F00001093

- (1) Have a system of records;
- (2) Create, collect, use, process, store, maintain, disseminate, disclose, dispose or otherwise handle personally identifiable information; or
- (3) Design, develop, maintain, or operate a system of records.

(End of clause)

I.12 PERIOD OF PERFORMANCE (MAR 2003)

The period of performance of this contract shall be from 9/21/2018 through 9/20/2019.

[End of Clause]

I.13 CONTRACTING OFFICER'S AUTHORITY (MAR 2003)

The Contracting Officer is the only person authorized to approve changes in any of the requirements of this contract. In the event the Contractor effects any changes at the direction of any person other than the Contracting Officer, the changes will be considered to have been made without authority and no adjustment will be made in the contract price to cover any increase in costs incurred as a result thereof. The Contracting Officer shall be the only individual authorized to accept nonconforming work, waive any requirement of the contract, or to modify any term or condition of the contract. The Contracting Officer is the only individual who can legally obligate Government funds. No cost chargeable to the proposed contract can be incurred before receipt of a fully executed contract or specific authorization from the Contracting Officer.

[End of Clause]

I.14 ELECTRONIC INVOICING AND PAYMENT REQUIREMENTS - INVOICE PROCESSING PLATFORM (IPP) (JAN 2016)

Beginning April 11, 2016, payment requests for all new awards must be submitted electronically through the U. S. Department of the Treasury's Invoice Processing Platform System (IPP). Payment terms for existing contracts and orders awarded prior to April 11, 2016 remain the same. The Contractor must use IPP for contracts and orders awarded April 11, 2016 or later, and must use the non-IPP invoicing process for those contracts and orders awarded prior to April 11, 2016.

"Payment request" means any request for contract financing payment or invoice payment by the Contractor. To constitute a proper invoice, the payment request must comply with the requirements identified in FAR 32.905(b), "Payment documentation and process" and the applicable Prompt Payment clause included in this contract. The IPP website address is: <https://www.ipp.gov>.

Under this contract, the following documents are required to be submitted as an attachment to the IPP:

- _____
- _____
- _____
- _____
- _____

The IPP was designed and developed for Contractors to enroll, access and use IPP for submitting requests for payment. Contractor assistance with enrollment can be obtained by contacting IPPCustomerSupport@fms.treas.gov or phone (866) 973-3131.

If the Contractor is unable to comply with the requirement to use IPP for submitting invoices for payment, the Contractor must submit a waiver request in writing to the contracting officer.

(End of Clause)

I.15 GOVERNMENT CONSENT OF PUBLICATION/ENDORSEMENT (MAR 2003)

70B04C18F00001093

Under no circumstances shall the Contractor, or anyone acting on behalf of the Contractor, refer to the supplies, services, or equipment furnished pursuant to the provisions of this contract in any news release or commercial advertising without first obtaining explicit written consent to do so from the Contracting Officer

The Contractor agrees not to refer to awards in commercial advertising in such a manner as to state or imply that the product or service provided is endorsed or preferred by the Federal Government or is considered by the Government to be superior to other products or services.

[End of Clause]

I.16 SECURITY PROCEDURES (OCT 2009)

A. Controls

1. The Contractor shall comply with the U.S. Customs and Border Protection (CBP) administrative, physical and technical security controls to ensure that the Government's security requirements are met.
2. All Government furnished information must be protected to the degree and extent required by local rules, regulations, and procedures. The Contractor shall comply with all security policies contained in CBP Handbook 1400-05C, Information Systems Security Policies and Procedures Handbook.
3. All services provided under this contract must be compliant with the Department of Homeland Security (DHS) information security policy identified in DHS Management Directive (MD) 4300.1, Information Technology Systems Security Program and DHS 4300A, Sensitive Systems Handbook.
4. All Contractor employees under this contract must wear identification access badges when working in CBP facilities. Prior to Contractor employees' departure/separation, all badges, building passes, parking permits, keys and pass cards must be given to the Contracting Officer's Technical Representative (COTR). The COTR will ensure that the cognizant Physical Security official is notified so that access to all buildings and facilities can be revoked. NOTE: For contracts within the National Capitol Region (NCR), the Office of Internal Affairs, Security Management Division (IA/SMD) should be notified if building access is revoked.
5. All Contractor employees must be registered in the Contractor Tracking System (CTS) database by the Contracting Officer (CO) or COTR. The Contractor shall provide timely start information to the CO/COTR or designated government personnel to initiate the CTS registration. Other relevant information will also be needed for registration in the CTS database such as, but not limited to, the contractor's legal name, address, brief job description, labor rate, Hash ID, schedule and contract specific information. The CO/COTR or designated government personnel shall provide the Contractor with instructions for receipt of CTS registration information. Additionally, the CO/COTR shall immediately notify IA/SMD of the contractor's departure/separation.
6. The Contractor shall provide employee departure/separation date and reason for leaving to the CO/COTR in accordance with CBP Directive 51715-006, Separation Procedures for Contractor Employees. Failure by the Contractor to provide timely notification of employee departure/separation in accordance with the contract requirements shall be documented and considered when government personnel completes a Contractor Performance Report (under Business Relations) or other performance related measures.

B. Security Background Investigation Requirements

1. In accordance with DHS Management Directive (MD) 11055, Suitability Screening Requirements for Contractors, Part VI, Policy and Procedures, Section E, Citizenship and Residency Requirements, contractor employees who require access to sensitive information must be U.S. citizens or have Lawful Permanent Resident (LPR) status. A waiver may be granted, as outlined in MD 11055, Part VI, Section M (1).
2. Contractor employees that require access to DHS IT systems or development, management, or maintenance of those systems must be U.S. citizens in accordance with MD 11055, Part VI, Section E (Lawful Permanent Resident status is not acceptable in this case). A waiver may be granted, as outlined in MD 11055, Part VI, Section M (2)
3. Provided the requirements of DHS MD 11055 are met as outlined in paragraph 1, above, contractor employees requiring access to CBP facilities, sensitive information or information technology resources are required to have a favorably adjudicated background investigation (BI) or a single scope background investigation (SSBI) prior to commencing work on this contract. Exceptions shall be approved on a case-by-case basis with the employee's

70B04C18F00001093

access to facilities, systems, and information limited until the Contractor employee receives a favorably adjudicated BI or SSBI. A favorable adjudicated BI or SSBI shall include various aspects of a Contractor employee's life, including employment, education, residences, police and court inquiries, credit history, national agency checks, and a CBP Background Investigation Personal Interview (BIPi).

4. The Contractor shall submit within ten (10) working days after award of this contract a list containing the full name, social security number, place of birth (city and state), and date of birth of employee candidates who possess favorably adjudicated BI or SSBI that meets federal investigation standards.. For employee candidates needing a BI for this contract, the Contractor shall require the applicable employees to submit information and documentation requested by CBP to initiate the BI process.
5. Background Investigation information and documentation is usually submitted by completion of standard federal and agency forms such as Questionnaire for Public Trust and Selected Positions or Questionnaire for National Security Positions; Fingerprint Chart; Fair Credit Reporting Act (FCRA) form; Criminal History Request form; and Financial Disclosure form. These forms must be submitted to the designated CBP official identified in this contract. The designated CBP security official will review the information for completeness.
6. The estimated completion of a BI or SSBI is approximately sixty (60) to ninety (90) days from the date of receipt of the properly completed forms by CBP security office. During the term of this contract, the Contractor is required to provide the names of contractor employees who successfully complete the CBP BI or SSBI process. Failure of any contractor employee to obtain and maintain a favorably adjudicated BI or SSBI shall be cause for dismissal. For key personnel, the Contractor shall propose a qualified replacement employee candidate to the CO and COTR within 30 days after being notified of an unsuccessful candidate or vacancy. For all non-key personnel contractor employees, the Contractor shall propose a qualified replacement employee candidate to the COTR within 30 days after being notified of an unsuccessful candidate or vacancy. The CO/COTR shall approve or disapprove replacement employees. Continuous failure to provide contractor employees who meet CBP BI or SSBI requirements may be cause for termination of the contract.

C. Security Responsibilities

1. The Contractor shall ensure that its employees follow the general procedures governing physical, environmental, and information security described in the various DHS CBP regulations identified in this clause. The contractor shall ensure that its employees apply proper business practices in accordance with the specifications, directives, and manuals required for conducting work under this contract. Applicable contractor personnel will be responsible for physical security of work areas and CBP furnished equipment issued under this contract.
2. The CO/COTR may require the Contractor to prohibit its employees from working on this contract if continued employment becomes detrimental to the public's interest for any reason including, but not limited to carelessness, insubordination, incompetence, or security concerns.
3. Work under this contract may require access to sensitive information as defined under Homeland Security Acquisition Regulation (HSAR) Clause 3052.204-71, Contractor Employee Access, included in the solicitation/contract. The Contractor shall not disclose, orally or in writing, any sensitive information to any person unless authorized in writing by the CO.
4. The Contractor shall ensure that its employees who are authorized access to sensitive information, receive training pertaining to protection and disclosure of sensitive information. The training shall be conducted during and after contract performance.
5. Upon completion of this contract, the Contractor shall return all sensitive information used in the performance of the contract to the CO/COTR. The Contractor shall certify, in writing, that all sensitive and non-public information has been purged from any Contractor-owned system.

D. Notification of Contractor Employee Changes

1. The Contractor shall notify the CO/COTR via phone, facsimile, or electronic transmission, immediately after a personnel change become known or no later than five (5) business days prior to departure of the employee. Telephone notifications must be immediately followed up in writing. Contractor's notification shall include, but is not limited to name changes, resignations, terminations, and reassignments to another contract.

70B04C18F00001093

2. The Contractor shall notify the CO/COTR and program office (if applicable) in writing of any proposed change in access requirements for its employees at least fifteen (15) days, or thirty (30) days if a security clearance is to be obtained, in advance of the proposed change. The CO/COTR will notify the Office of Information and Technology (OIT) Information Systems Security Branch (ISSB) of the proposed change. If a security clearance is required, the CO/COTR will notify IA/SMD.

E. Non-Disclosure Agreements

When determined to be appropriate, Contractor employees are required to execute a non-disclosure agreement (DHS Form 11000-6) as a condition to access sensitive but unclassified information.

[End of Clause]

I.17 SPECIAL SECURITY REQUIREMENT - CONTRACTOR PRE-SCREENING (SEP 2011)

1. Contractors requiring recurring access to Government facilities or access to sensitive but unclassified information and/or logical access to Information Technology (IT) resources shall verify minimal fitness requirements for all persons/candidates designated for employment under any Department of Security (DHS) contract by pre-screening the person /candidate prior to submitting the name for consideration to work on the contract. Pre-screening the candidate ensures that minimum fitness requirements are considered and mitigates the burden of DHS having to conduct background investigations on objectionable candidates. The Contractor shall submit only those candidates that have not had a felony conviction within the past 36 months or illegal drug use within the past 12 months from the date of submission of their name as a candidate to perform work under this contract. Contractors are required to flow this requirement down to subcontractors. Pre-screening involves contractors and subcontractors reviewing:
 - a. Felony convictions within the past 36 months. An acceptable means of obtaining information on felony convictions is from public records, free of charge, or from the National Crime Information Center (NCIC).
 - b. Illegal drug use within the past 12 months. An acceptable means of obtaining information related to drug use is through employee self certification, by public records check; or if the contractor or subcontractor already has drug testing in place. There is no requirement for contractors and/or subcontractors to initiate a drug testing program if they do not have one already in place.
 - c. Misconduct such as criminal activity on the job relating to fraud or theft within the past 12 months. An acceptable means of obtaining information related to misconduct is through employee self certification, by public records check, or other reference checks conducted in the normal course of business.
2. Pre-screening shall be conducted within 15 business days after contract award. This requirement shall be placed in all subcontracts if the subcontractor requires routine physical access, access to sensitive but unclassified information, and/or logical access to IT resources. Failure to comply with the pre-screening requirement will result in the Contracting Officer taking the appropriate remedy.

Definition: *Logical Access* means providing an authorized user the ability to access one or more computer system resources such as a workstation, network, application, or database through automated tools. A logical access control system (LACS) requires validation of an individual identity through some mechanism such as a personal identification number (PIN), card, username and password, biometric, or other token. The system has the capability to assign different access privileges to different persons depending on their roles and responsibilities in an organization.

[End of Clause]

ORDER FOR SUPPLIES OR SERVICES

PAGE OF PAGES

1 8

IMPORTANT: Mark all packages and papers with contract and/or order numbers.

| 1. DATE OF ORDER 9/20/2018 | | 2. CONTRACT NO. (if any) HSHQDC-12-D-00013 | | 6. SHIP TO: | | |
|---|--------------------------|---|----------|--|------------|-------------------------------------|
| 3. ORDER NO. 70B04C18F00001093 | | 4. REQUISITION/REFERENCE NO. 0020099198 | | a. NAME OF CONSIGNEE See Attached Delivery Schedule | | |
| 5. ISSUING OFFICE (Address correspondence to) DHS - Customs & Border Protection Customs and Border Protection 1300 Pennsylvania Ave, NW Procurement Directorate - NP 1310 Washington DC 20229 | | | | b. STREET ADDRESS | | |
| c. CITY | | d. STATE | | e. ZIP CODE | | |
| 7. TO: | | | | f. SHIP VIA | | |
| a. NAME OF CONTRACTOR PANAMERICA COMPUTERS, INC. | | | | 8. TYPE OF ORDER | | |
| b. COMPANY NAME | | | | <input type="checkbox"/> a. PURCHASE -- Reference Your BID # 565079305. Please furnish the following on the terms and conditions specified on both sides of this order and on the attached sheet, if any, including delivery as indicated. | | |
| c. STREET ADDRESS 1386 BIG OAK RD. | | | | <input checked="" type="checkbox"/> b. DELIVERY -- Except for billing instructions on the reverse, this delivery order is subject to instructions contained on this side only of this form and is issued subject to the terms and conditions of the above-numbered contract. | | |
| d. CITY LURAY | | e. STATE VA | | f. ZIP CODE 22835 | | |
| 9. ACCOUNTING AND APPROPRIATION DATA | | | | 10. REQUISITIONING OFFICE (b) (6), (b) (7)(C) | | |
| 11. BUSINESS CLASSIFICATION (Check appropriate box(es)) | | | | | | 12. F.O.B. POINT |
| <input checked="" type="checkbox"/> a. SMALL <input type="checkbox"/> b. OTHER THAN SMALL <input type="checkbox"/> c. DISADVANTAGED <input type="checkbox"/> d. WOMEN-OWNED <input checked="" type="checkbox"/> e. HUBZone <input type="checkbox"/> f. SERVICE-DISABLED VETERAN-OWNED <input type="checkbox"/> g. WOMEN-OWNED SMALL BUSINESS (WOSB) ELIGIBLE UNDER THE WOSB PROGRAM <input type="checkbox"/> h. ECONOMICALLY DISADVANTAGED WOMEN-OWNED SMALL BUSINESS (EDWOSB) | | | | | | Not applicable |
| 13. PLACE OF | | 14. GOVERNMENT B/L NO. | | 15. DELIVER TO F.O.B POINT ON OR BEFORE (Date) | | 16. DISCOUNT TERMS |
| a. INSPECTION | | b. ACCEPTANCE | | 09/21/2018 | | Within 30 days Due net |
| 17. SCHEDULE (See reverse for Rejections) | | | | | | |
| ITEM NO. (a) | SUPPLIES OR SERVICES (b) | QUANTITY ORDERED (c) | UNIT (d) | UNIT PRICE (e) | AMOUNT (f) | Accept |
| 10 | (b) (7)(E) | 1.000 | EA | (b) (4) | | |
| 18. SHIPPING POINT | | 19. GROSS SHIPPING WEIGHT | | 20. INVOICE NO. | | |
| 21. MAIL INVOICE TO: | | | | | | 17(h)TOT. (Cont. pages) |
| a. NAME DHS - Customs & Border Protection | | Commercial Accounts Sect. | | | | \$0.00 |
| b. STREET ADDRESS (or P.O. Box) 6650 Telecom Drive, Suite 100 | | | | | | 17(i) GRAND TOTAL |
| c. CITY Indianapolis | | d. STATE IN | | e. ZIP CODE 46278 | | |
| 22. UNITED STATES OF AMERICA BY (Signature) | | (b) (6), (b) (7)(C) | | 23. NAME (Type) (b) (6), (b) (7)(C) | | |
| | | | | | | TITLE: CONTRACTING/ORDERING OFFICER |

AUTHORIZED FOR LOCAL REPRODUCTION
PREVIOUS EDITION NOT USABLE

| | | | |
|----------------------------|--|--------------------------------|----------------------|
| DATE OF ORDER 9/20/2018 | CONTRACT NO. (if any) HSHQDC-12-D-00013 | ORDER NO. 70B04C18F00001093 | PAGE OF PAGES 2 8 |
|----------------------------|--|--------------------------------|----------------------|

Federal Tax Exempt ID: (b) (3) (A)

Emailing Invoices to CBP. Do not mail or email invoices to CBP. Invoices must be submitted via the IPP website, as detailed under Electronic Invoicing and Payment Requirements in the attached terms and conditions.

NOTES:

This Firm Fixed Price delivery order, 70B04C18F00001093, is issued against the Department of Homeland Security FirstSource II Contract HSHQDC-12-D-00013 for (b) (7)(E) Licenses and Maintenance in support of (b) (7)(E) (b) (7)(E). The Statement of Work will be provided with the Award Distribution email.

Reference Bid # 565079305, dated 9/05/2018, from FedBid Buy #945260_01

The Period of Performance for 70B04C18F00001093 will be [REDACTED]

The Contracting Officer's Representative for this order is:

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

Address: (b) (7)(E)

(b) (7)(E)

Tel. #: (b) (6), (b) (7)(C)

Fax #:

(b) (6), (b) (7)(C) @cbp.dhs.gov

Invoices shall be sent to:

IPP.gov in accordance with Section 10.5 of the SOW.

All Terms and Conditions of the FirstSource II Contract HSHQDC-12-D-00013 are in full force and effect.

70B04C18F00001093

**ITEMS AND PRICES, DELIVERY SCHEDULE AND ACCOUNTING DATA
FOR
DELIVERY ORDER: 70B04C18F00001093**

I.1 SCHEDULE OF SUPPLIES/SERVICES

| ITEM # | DESCRIPTION | QTY | UNIT | UNIT PRICE | EXT. PRICE |
|--------|-------------|-------|------|------------|------------|
| 10 | (b) (7)(E) | 1.000 | EA | (b) (4) | |

Total Funded Value of Award:

\$2,206,058.25

I.2 ACCOUNTING and APPROPRIATION DATA

| ITEM # | ACCOUNTING and APPROPRIATION DATA | AMOUNT |
|--------|--|----------------|
| 10 | 6100.315BUSCSGLCS0942715000Z00018500TT0600000000 IU549315B TAS# 07020182018 0530000 | \$2,206,058.25 |

I.3 DELIVERY SCHEDULE

| DELIVER TO: | ITEM # | QTY | DELIVERY DATE |
|---|--------|-------|---------------|
| Customs and Border Protection (b) (7)(E) | 10 | 1.000 | (b) (7)(E) |

I.4 52.232-39 UNENFORCEABILITY OF UNAUTHORIZED OBLIGATIONS (JUN 2013)

(a) Except as stated in paragraph (b) of this clause, when any supply or service acquired under this contract is subject to any End User License Agreement (EULA), Terms of Service (TOS), or similar legal instrument or agreement, that includes any clause requiring the Government to indemnify the Contractor or any person or entity for damages, costs, fees, or any other loss or liability that would create an Anti-Deficiency Act violation (31 U.S.C. 1341), the following shall govern:

(1) Any such clause is unenforceable against the Government.

(2) Neither the Government nor any Government authorized end user shall be deemed to have agreed to such clause by virtue of it appearing in the EULA, TOS, or similar legal instrument or agreement. If the EULA, TOS, or similar legal instrument or agreement is invoked through an "I agree" click box or other comparable mechanism (e.g., "click-wrap" or "browse-wrap" agreements), execution does not bind the Government or any Government authorized end user to such clause.

(3) Any such clause is deemed to be stricken from the EULA, TOS, or similar legal instrument or agreement.

(b) Paragraph (a) of this clause does not apply to indemnification by the Government that is expressly authorized by statute and specifically authorized under applicable agency regulations and procedures.

(End of clause)

I.5 52.232-40 PROVIDING ACCELERATED PAYMENTS TO SMALL BUSINESS SUBCONTRACTORS (DEC 2013)

(a) Upon receipt of accelerated payments from the Government, the Contractor shall make accelerated payments to its small business subcontractors under this contract, to the maximum extent practicable and prior to when such payment is otherwise required under the applicable contract or subcontract, after receipt of a proper invoice and all other required documentation from the small business subcontractor.

(b) The acceleration of payments under this clause does not provide any new rights under the Prompt Payment Act.

(c) Include the substance of this clause, including this paragraph (c), in all subcontracts with small business concerns, including subcontracts with small business concerns for the acquisition of commercial items.

70B04C18F00001093

(End of clause)

I.6 52.203-19 PROHIBITION ON REQUIRING CERTAIN INTERNAL CONFIDENTIALITY AGREEMENTS OR STATEMENTS (JAN 2017)

I.7 52.204-22 ALTERNATIVE LINE ITEM PROPOSAL (JAN 2017)

I.8 52.204-23 - PROHIBITION ON CONTRACTING FOR HARDWARE, SOFTWARE, AND SERVICES DEVELOPED OR PROVIDED BY KASPERSKY LAB AND OTHER COVERED ENTITIES (JUL 2018)

I.9 52.209-10 PROHIBITION ON CONTRACTING WITH INVERTED DOMESTIC CORPORATIONS (NOV 2015)

I.10 3052.205-70 ADVERTISEMENTS, PUBLICIZING AWARDS, AND RELEASES (SEP 2012) ALTERNATE I (SEP 2012)

- (a) The Contractor shall not refer to this contract in commercial advertising or similar promotions in such a manner as to state or imply that the product or service provided is endorsed or preferred by the Federal Government or is considered by the Government to be superior to other products or services.
- (b) All advertisements, releases, announcements, or other publication regarding this contract or the agency programs and projects covered under it, or the results or conclusions made pursuant to performance, must be approved by the Contracting Officer. Under no circumstances shall the Contractor, or anyone acting on behalf of the Contractor, refer to the supplies, services, or equipment furnished pursuant to the provisions of this contract in any publicity, release, or commercial advertising without first obtaining explicit written consent to do so from the Contracting Officer.

(End of clause)

I.11 52.224-3 PRIVACY TRAINING, ALTERNATE I (DEVIATION)

- (a) Definition. As used in this clause, personally identifiable information means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. (See Office of Management and Budget (OMB) *Circular A-130, Managing Federal Information as a Strategic Resource*).
- (b) The Contractor shall ensure that initial privacy training, and annual privacy training thereafter, is completed by contractor employees who--
 - (1) Have access to a system of records;
 - (2) Create, collect, use, process, store, maintain, disseminate, disclose, dispose, or otherwise handle personally identifiable information on behalf of an agency; or
 - (3) Design, develop, maintain, or operate a system of records (see also FAR subpart 24.1 and 39.105).
- (c) The contracting agency will provide initial privacy training, and annual privacy training thereafter, to Contractor employees for the duration of this contract. Contractor employees shall satisfy this requirement by completing *Privacy at DHS: Protecting Personal Information* accessible at <http://www.dhs.gov/dhs-security-and-training-requirements-contractors>. Training shall be completed within 30 days of contract award and be completed on an annual basis thereafter not later than October 31st of each year.
- (d) The Contractor shall maintain and, upon request, provide documentation of completion of privacy training to the Contracting Officer.
- (e) The Contractor shall not allow any employee access to a system of records, or permit any employee to create, collect, use, process, store, maintain, disseminate, disclose, dispose or otherwise handle personally identifiable information, or to design, develop, maintain, or operate a system of records unless the employee has completed privacy training, as required by this clause.
- (f) The substance of this clause, including this paragraph (f), shall be included in all subcontracts under this contract, when subcontractor employees will –

70B04C18F00001093

- (1) Have a system of records;
- (2) Create, collect, use, process, store, maintain, disseminate, disclose, dispose or otherwise handle personally identifiable information; or
- (3) Design, develop, maintain, or operate a system of records.

(End of clause)

I.12 PERIOD OF PERFORMANCE (MAR 2003)

The period of performance of this contract shall be from 9/21/2018 through 9/20/2019.

[End of Clause]

I.13 CONTRACTING OFFICER'S AUTHORITY (MAR 2003)

The Contracting Officer is the only person authorized to approve changes in any of the requirements of this contract. In the event the Contractor effects any changes at the direction of any person other than the Contracting Officer, the changes will be considered to have been made without authority and no adjustment will be made in the contract price to cover any increase in costs incurred as a result thereof. The Contracting Officer shall be the only individual authorized to accept nonconforming work, waive any requirement of the contract, or to modify any term or condition of the contract. The Contracting Officer is the only individual who can legally obligate Government funds. No cost chargeable to the proposed contract can be incurred before receipt of a fully executed contract or specific authorization from the Contracting Officer.

[End of Clause]

I.14 ELECTRONIC INVOICING AND PAYMENT REQUIREMENTS - INVOICE PROCESSING PLATFORM (IPP) (JAN 2016)

Beginning April 11, 2016, payment requests for all new awards must be submitted electronically through the U. S. Department of the Treasury's Invoice Processing Platform System (IPP). Payment terms for existing contracts and orders awarded prior to April 11, 2016 remain the same. The Contractor must use IPP for contracts and orders awarded April 11, 2016 or later, and must use the non-IPP invoicing process for those contracts and orders awarded prior to April 11, 2016.

"Payment request" means any request for contract financing payment or invoice payment by the Contractor. To constitute a proper invoice, the payment request must comply with the requirements identified in FAR 32.905(b), "Payment documentation and process" and the applicable Prompt Payment clause included in this contract. The IPP website address is: <https://www.ipp.gov>.

Under this contract, the following documents are required to be submitted as an attachment to the IPP:

- _____
- _____
- _____
- _____
- _____

The IPP was designed and developed for Contractors to enroll, access and use IPP for submitting requests for payment. Contractor assistance with enrollment can be obtained by contacting IPPCustomerSupport@fms.treas.gov or phone (866) 973-3131.

If the Contractor is unable to comply with the requirement to use IPP for submitting invoices for payment, the Contractor must submit a waiver request in writing to the contracting officer.

(End of Clause)

I.15 GOVERNMENT CONSENT OF PUBLICATION/ENDORSEMENT (MAR 2003)

70B04C18F00001093

Under no circumstances shall the Contractor, or anyone acting on behalf of the Contractor, refer to the supplies, services, or equipment furnished pursuant to the provisions of this contract in any news release or commercial advertising without first obtaining explicit written consent to do so from the Contracting Officer

The Contractor agrees not to refer to awards in commercial advertising in such a manner as to state or imply that the product or service provided is endorsed or preferred by the Federal Government or is considered by the Government to be superior to other products or services.

[End of Clause]

I.16 SECURITY PROCEDURES (OCT 2009)

A. Controls

1. The Contractor shall comply with the U.S. Customs and Border Protection (CBP) administrative, physical and technical security controls to ensure that the Government's security requirements are met.
2. All Government furnished information must be protected to the degree and extent required by local rules, regulations, and procedures. The Contractor shall comply with all security policies contained in CBP Handbook 1400-05C, Information Systems Security Policies and Procedures Handbook.
3. All services provided under this contract must be compliant with the Department of Homeland Security (DHS) information security policy identified in DHS Management Directive (MD) 4300.1, Information Technology Systems Security Program and DHS 4300A, Sensitive Systems Handbook.
4. All Contractor employees under this contract must wear identification access badges when working in CBP facilities. Prior to Contractor employees' departure/separation, all badges, building passes, parking permits, keys and pass cards must be given to the Contracting Officer's Technical Representative (COTR). The COTR will ensure that the cognizant Physical Security official is notified so that access to all buildings and facilities can be revoked. NOTE: For contracts within the National Capitol Region (NCR), the Office of Internal Affairs, Security Management Division (IA/SMD) should be notified if building access is revoked.
5. All Contractor employees must be registered in the Contractor Tracking System (CTS) database by the Contracting Officer (CO) or COTR. The Contractor shall provide timely start information to the CO/COTR or designated government personnel to initiate the CTS registration. Other relevant information will also be needed for registration in the CTS database such as, but not limited to, the contractor's legal name, address, brief job description, labor rate, Hash ID, schedule and contract specific information. The CO/COTR or designated government personnel shall provide the Contractor with instructions for receipt of CTS registration information. Additionally, the CO/COTR shall immediately notify IA/SMD of the contractor's departure/separation.
6. The Contractor shall provide employee departure/separation date and reason for leaving to the CO/COTR in accordance with CBP Directive 51715-006, Separation Procedures for Contractor Employees. Failure by the Contractor to provide timely notification of employee departure/separation in accordance with the contract requirements shall be documented and considered when government personnel completes a Contractor Performance Report (under Business Relations) or other performance related measures.

B. Security Background Investigation Requirements

1. In accordance with DHS Management Directive (MD) 11055, Suitability Screening Requirements for Contractors, Part VI, Policy and Procedures, Section E, Citizenship and Residency Requirements, contractor employees who require access to sensitive information must be U.S. citizens or have Lawful Permanent Resident (LPR) status. A waiver may be granted, as outlined in MD 11055, Part VI, Section M (1).
2. Contractor employees that require access to DHS IT systems or development, management, or maintenance of those systems must be U.S. citizens in accordance with MD 11055, Part VI, Section E (Lawful Permanent Resident status is not acceptable in this case). A waiver may be granted, as outlined in MD 11055, Part VI, Section M (2)
3. Provided the requirements of DHS MD 11055 are met as outlined in paragraph 1, above, contractor employees requiring access to CBP facilities, sensitive information or information technology resources are required to have a favorably adjudicated background investigation (BI) or a single scope background investigation (SSBI) prior to commencing work on this contract. Exceptions shall be approved on a case-by-case basis with the employee's

70B04C18F00001093

access to facilities, systems, and information limited until the Contractor employee receives a favorably adjudicated BI or SSBI. A favorable adjudicated BI or SSBI shall include various aspects of a Contractor employee's life, including employment, education, residences, police and court inquiries, credit history, national agency checks, and a CBP Background Investigation Personal Interview (BIPi).

4. The Contractor shall submit within ten (10) working days after award of this contract a list containing the full name, social security number, place of birth (city and state), and date of birth of employee candidates who possess favorably adjudicated BI or SSBI that meets federal investigation standards.. For employee candidates needing a BI for this contract, the Contractor shall require the applicable employees to submit information and documentation requested by CBP to initiate the BI process.
5. Background Investigation information and documentation is usually submitted by completion of standard federal and agency forms such as Questionnaire for Public Trust and Selected Positions or Questionnaire for National Security Positions; Fingerprint Chart; Fair Credit Reporting Act (FCRA) form; Criminal History Request form; and Financial Disclosure form. These forms must be submitted to the designated CBP official identified in this contract. The designated CBP security official will review the information for completeness.
6. The estimated completion of a BI or SSBI is approximately sixty (60) to ninety (90) days from the date of receipt of the properly completed forms by CBP security office. During the term of this contract, the Contractor is required to provide the names of contractor employees who successfully complete the CBP BI or SSBI process. Failure of any contractor employee to obtain and maintain a favorably adjudicated BI or SSBI shall be cause for dismissal. For key personnel, the Contractor shall propose a qualified replacement employee candidate to the CO and COTR within 30 days after being notified of an unsuccessful candidate or vacancy. For all non-key personnel contractor employees, the Contractor shall propose a qualified replacement employee candidate to the COTR within 30 days after being notified of an unsuccessful candidate or vacancy. The CO/COTR shall approve or disapprove replacement employees. Continuous failure to provide contractor employees who meet CBP BI or SSBI requirements may be cause for termination of the contract.

C. Security Responsibilities

1. The Contractor shall ensure that its employees follow the general procedures governing physical, environmental, and information security described in the various DHS CBP regulations identified in this clause. The contractor shall ensure that its employees apply proper business practices in accordance with the specifications, directives, and manuals required for conducting work under this contract. Applicable contractor personnel will be responsible for physical security of work areas and CBP furnished equipment issued under this contract.
2. The CO/COTR may require the Contractor to prohibit its employees from working on this contract if continued employment becomes detrimental to the public's interest for any reason including, but not limited to carelessness, insubordination, incompetence, or security concerns.
3. Work under this contract may require access to sensitive information as defined under Homeland Security Acquisition Regulation (HSAR) Clause 3052.204-71, Contractor Employee Access, included in the solicitation/contract. The Contractor shall not disclose, orally or in writing, any sensitive information to any person unless authorized in writing by the CO.
4. The Contractor shall ensure that its employees who are authorized access to sensitive information, receive training pertaining to protection and disclosure of sensitive information. The training shall be conducted during and after contract performance.
5. Upon completion of this contract, the Contractor shall return all sensitive information used in the performance of the contract to the CO/COTR. The Contractor shall certify, in writing, that all sensitive and non-public information has been purged from any Contractor-owned system.

D. Notification of Contractor Employee Changes

1. The Contractor shall notify the CO/COTR via phone, facsimile, or electronic transmission, immediately after a personnel change become known or no later than five (5) business days prior to departure of the employee. Telephone notifications must be immediately followed up in writing. Contractor's notification shall include, but is not limited to name changes, resignations, terminations, and reassignments to another contract.

70B04C18F00001093

2. The Contractor shall notify the CO/COTR and program office (if applicable) in writing of any proposed change in access requirements for its employees at least fifteen (15) days, or thirty (30) days if a security clearance is to be obtained, in advance of the proposed change. The CO/COTR will notify the Office of Information and Technology (OIT) Information Systems Security Branch (ISSB) of the proposed change. If a security clearance is required, the CO/COTR will notify IA/SMD.

E. Non-Disclosure Agreements

When determined to be appropriate, Contractor employees are required to execute a non-disclosure agreement (DHS Form 11000-6) as a condition to access sensitive but unclassified information.

[End of Clause]

I.17 SPECIAL SECURITY REQUIREMENT - CONTRACTOR PRE-SCREENING (SEP 2011)

1. Contractors requiring recurring access to Government facilities or access to sensitive but unclassified information and/or logical access to Information Technology (IT) resources shall verify minimal fitness requirements for all persons/candidates designated for employment under any Department of Security (DHS) contract by pre-screening the person /candidate prior to submitting the name for consideration to work on the contract. Pre-screening the candidate ensures that minimum fitness requirements are considered and mitigates the burden of DHS having to conduct background investigations on objectionable candidates. The Contractor shall submit only those candidates that have not had a felony conviction within the past 36 months or illegal drug use within the past 12 months from the date of submission of their name as a candidate to perform work under this contract. Contractors are required to flow this requirement down to subcontractors. Pre-screening involves contractors and subcontractors reviewing:
 - a. Felony convictions within the past 36 months. An acceptable means of obtaining information on felony convictions is from public records, free of charge, or from the National Crime Information Center (NCIC).
 - b. Illegal drug use within the past 12 months. An acceptable means of obtaining information related to drug use is through employee self certification, by public records check; or if the contractor or subcontractor already has drug testing in place. There is no requirement for contractors and/or subcontractors to initiate a drug testing program if they do not have one already in place.
 - c. Misconduct such as criminal activity on the job relating to fraud or theft within the past 12 months. An acceptable means of obtaining information related to misconduct is through employee self certification, by public records check, or other reference checks conducted in the normal course of business.
2. Pre-screening shall be conducted within 15 business days after contract award. This requirement shall be placed in all subcontracts if the subcontractor requires routine physical access, access to sensitive but unclassified information, and/or logical access to IT resources. Failure to comply with the pre-screening requirement will result in the Contracting Officer taking the appropriate remedy.

Definition: *Logical Access* means providing an authorized user the ability to access one or more computer system resources such as a workstation, network, application, or database through automated tools. A logical access control system (LACS) requires validation of an individual identity through some mechanism such as a personal identification number (PIN), card, username and password, biometric, or other token. The system has the capability to assign different access privileges to different persons depending on their roles and responsibilities in an organization.

[End of Clause]

Award 70B04C18F00001257
Statement of Work
Department of Homeland Security
Customs & Border Protection (CBP)
(b) (7)(E)

1.0 General

In support of US Customs and Border Protection (CBP) mission of securing our nation’s borders, the (b) (7)(E) has a need to procure (b) (7)(E) to ensure employees have the continued ability to (b) (7)(E)

This software will be utilized by users across CBP as a replacement for the Department of Homeland Security (DHS) (b) (7)(E).

1.1 Scope

The purpose of this order is for the contractor to provide the following software:

| Item Description | Quantity |
|------------------|------------|
| (b) (7)(E) | (b) (7)(E) |

2.0 Period of Performance

The period of performance for this contract will be Date of Award – 12 Month. Delivery within 30 days of award.

3.0 Place of Performance

Location: All work required under this order shall be performed by the contractor at Government sites unless otherwise directed by the Government.

4.0 Deliverables

The contractor shall provide the following deliverables:

| Deliverable | Due |
|-------------|---------------|
| (b) (7)(E) | Date of Award |

| | |
|------------|---------------|
| (b) (7)(E) | Date of Award |
| | Date of Award |
| | Date of Award |

4.1 Personally Identifiable Information (PII)

When a contractor, on the behalf of CBP, handles Sensitive PII data, stores and transmits, the contractor will Accredited (ATO) this information system to the High, High, Moderate (HHM) FIPS level.

5.0 Type of Contract

Customs and Border Protection will award a firm fixed price task order.

6.0 Invoicing and Payment

ELECTRONIC INVOICING AND PAYMENT REQUIREMENTS - INVOICE PROCESSING PLATFORM (IPP) (JAN 2016)

Beginning April 11, 2016, payment requests for all new awards must be submitted electronically through the U. S. Department of the Treasury's Invoice Processing Platform System (IPP). Payment terms for existing contracts and orders awarded prior to April 11, 2016 remain the same. The Contractor must use IPP for contracts and orders awarded April 11, 2016 or later, and must use the non-IPP invoicing process for those contracts and orders awarded prior to April 11, 2016.

"Payment request" means any request for contract financing payment or invoice payment by the Contractor. To constitute a proper invoice, the payment request must comply with the requirements identified in FAR 32.905(b), "Payment documentation and process" and the applicable Prompt Payment clause included in this contract. The IPP website address is: <https://www.ipp.gov>.

Under this contract, the following documents are required to be submitted as an attachment to the IPP invoice *[CO to edit and include the documentation required under this contract]*:

The IPP was designed and developed for Contractors to enroll, access and use IPP for submitting requests for payment. Contractor assistance with enrollment can be obtained by contacting IPPCustomerSupport@fms.treas.gov or phone (866) 973-3131.

If the Contractor is unable to comply with the requirement to use IPP for submitting invoices for payment, the Contractor must submit a waiver request in writing to the contracting officer.

(b) In accordance with FAR 32.904(b), the CO, in conjunction with the COR and NFC, will determine whether the invoice is proper or improper within seven (7) days of receipt. Improper invoices will be returned to the contractor within seven (7) days of receipt.

REVIEW AND APPROVAL REQUIREMENTS

(a) To constitute a proper invoice, invoices shall include, at a minimum, all the items required in FAR 32.905.

(1) The minimum requirements are:

- i. Name and address of the contractor.
- ii. Invoice date and invoice number.
- iii. Contract number or other authorization for supplies delivered or services performed (including order number and contract line item number.
- iv. Description, quantity, unit of measure, unit price, and extended price of supplies delivered or services performed.
- v. Shipping and payment terms (e.g. shipment number and date of shipment, discount for prompt payment terms). Bill of lading number and weight of shipment will be shown for shipments on Government bills of lading.
- vi. Name and address of contractor official to whom payment is to be sent (must be the same as that in the contract or in a proper notice of assignment).
- vii. Name (where practicable), title, phone number, and mailing address of person to notify in the event of a defective invoice.
- viii. Taxpayer identification number (TIN).
- ix. Electronic funds transfer (EFT) banking information.
- x. Any other information or documentation required by the contract (e.g. evidence of shipment).

(b) Supplemental documentation required for review and approval of invoices, at the written direction of the contracting officer, may be submitted directly to either the contracting officer, or the contracting officer's representative. Contractors shall submit all supplemental invoice documentation along with the original invoice.

(c) Invoices that fail to provide the information required by the Prompt Payment clause (FAR 52.232-25) may be rejected by the Government and returned to the contractor.

7.0 Point of Contact

CONTRACTING OFFICER'S REPRESENTATIVE

(b) (6), (b) (7)(C)

(b) (7)(E)

(b) (6), (b) (7)(C)

@cbp.dhs.gov

The Local Property Officer:

(b) (7)(C), (b) (6)

(b) (7)(E)

(b) (5), (b) (7)(C)

[\[REDACTED\]@cbp.dhs.gov](mailto: [REDACTED]@cbp.dhs.gov)

Only the contracting officer has the authority to represent the Government in cases where the task order requires a change in the terms and conditions, delivery schedule, scope of work and/or price of the products and/or services under this task order.

8.0 Clauses

The Clauses will be found in the Task Order award documents.

Enterprise Architecture (EA) Compliance

The Offeror shall ensure that the design conforms to the Department of Homeland Security (DHS) and Customs and Border Protection (CBP) Enterprise Architecture (EA), the DHS and CBP Technical Reference Models (TRM), and all DHS and CBP policies and guidelines (such as the CBP Information Technology Enterprise Principles and the [DHS Service Oriented Architecture - Technical Framework](#)), as promulgated by the DHS and CBP Chief Information Officers (CIO), Chief Technology Officers (CTO) and Chief Architects (CA).

The Offeror shall conform to the Federal Enterprise Architecture (FEA) model and the DHS and CBP versions of the FEA model, as described in their respective EAs. All models will be submitted using Business Process Modeling Notation (BPMN 1.1 or BPMN 2.0 when available) and the CBP Architectural Modeling Standards. Universal Modeling Language (UML2) may be used for infrastructure only. Data semantics shall be in conformance with the National Information Exchange Model (NIEM). Development solutions will also ensure compliance with the current version of the DHS and CBP target architectures.

Where possible, the Offeror shall use DHS/CBP approved products, standards, services, and profiles, as reflected by the hardware, software, application, and infrastructure components of the DHS/CBP TRM/standards profile. If new hardware, software, or infrastructure components are required to develop, test, or implement the program, these products will be coordinated through the DHS and CBP formal Technology Insertion (TI) process (to include a trade study with no less than four alternatives, one of which reflecting the status quo and another reflecting multi-agency collaboration). The DHS/CBP TRM/standards profile will be updated as TIs are resolved.

All developed solutions shall be compliant with the Homeland Security (HLS) EA.

All IT hardware and software shall be compliant with the HLS EA.

Compliance with the HLS EA shall be derived from and aligned through the CBP EA.

Description information for all data assets, information exchanges and data standards, whether adopted or developed, shall be submitted to the Enterprise Data Management Office (EDMO) for review, approval, and insertion into the DHS Data Reference Model and Enterprise Architecture Information Repository.

Development of data assets, information exchanges, and data standards will comply with the DHS Data Management Policy MD 103-01. All data-related artifacts will be developed and validated according to DHS Data Management Architectural Guidelines.

Applicability of Internet Protocol version 6 (IPv6) to DHS-related components (networks, infrastructure, and applications) specific to individual acquisitions shall be in accordance with the DHS EA (per OMB Memorandum M-05-22, August 2, 2005), regardless of whether the acquisition is for modification, upgrade, or replacement. All EA related component acquisitions shall be IPv6 compliant, as defined in the USGv6 Profile (NIST Special Publication 500-267) and the corresponding declarations of conformance, defined in the USGv6 Test Program.

Compliance with DHS Security Policy Terms and Conditions

All hardware, software, and services provided under this task order must be compliant with DHS 4300A DHS Sensitive System Policy and the DHS 4300A Sensitive Systems Handbook.

Encryption Compliance

If encryption is required, the following methods are acceptable for encrypting sensitive information:

1. FIPS 197 (Advanced Encryption Standard (AES)) 256 algorithm and cryptographic modules that have been validated under FIPS 140-2.
2. National Security Agency (NSA) Type 2 or Type 1 encryption.
3. Public Key Infrastructure (PKI) (see paragraph 5.5.2.1 of the Department of Homeland Security (DHS) IT Security Program Handbook (DHS Management Directive (MD) 4300A) for Sensitive Systems).

DHS Enterprise Architecture Compliance

All solutions and services shall meet DHS Enterprise Architecture policies, standards, and procedures. Specifically, the contractor shall comply with the following HLS EA requirements:

1. All developed solutions and requirements shall be compliant with the HLS EA.
2. All IT hardware and software shall be compliant with the HLS EA Technical Reference Model (TRM) Standards and Products Profile.
3. Description information for all data assets, information exchanges and data standards, whether adopted or developed, shall be submitted to the Enterprise Data Management Office (EDMO) for

review, approval and insertion into the DHS Data Reference Model and Enterprise Architecture Information Repository.

4. Development of data assets, information exchanges and data standards will comply with the DHS Data Management Policy MD 103-01 and all data-related artifacts will be developed and validated according to DHS data management architectural guidelines.
5. Applicability of Internet Protocol Version 6 (IPv6) to DHS-related components (networks, infrastructure, and applications) specific to individual acquisitions shall be in accordance with the DHS Enterprise Architecture (per OMB Memorandum M-05-22, August 2, 2005) regardless of whether the acquisition is for modification, upgrade, or replacement. All EA-related component acquisitions shall be IPv6 compliant as defined in the U.S. Government Version 6 (USGv6) Profile National Institute of Standards and Technology (NIST) Special Publication 500-267) and the corresponding declarations of conformance defined in the USGv6 Test Program.

Required Protections for DHS Systems Hosted in Non-DHS Data Centers

Security Authorization

A Security Authorization of any infrastructure directly in support of the DHS information system shall be performed as a general support system (GSS) prior to DHS occupancy to characterize the network, identify threats, identify vulnerabilities, analyze existing and planned security controls, determine likelihood of threat, analyze impact, determine risk, recommend controls, perform remediation on identified deficiencies, and document the results. The Security Authorization shall be performed in accordance with the DHS Security Policy and the controls provided by the hosting provider shall be equal to or stronger than the FIPS 199 security categorization of the DHS information system.

At the beginning of the contract, and annually thereafter, the contractor shall provide the results of an independent assessment and verification of security controls. The independent assessment and verification shall apply the same standards that DHS applies in the Security Authorization Process of its information systems. Any deficiencies noted during this assessment shall be provided to the COTR for entry into the DHS' Plan of Action and Milestone (POA&M) Management Process. The contractor shall use the DHS' POA&M process to document planned remedial actions to address any deficiencies in information security policies, procedures, and practices, and the completion of those activities. Security deficiencies shall be corrected within the timeframes dictated by the DHS POA&M Management Process. Contractor procedures shall be subject to periodic, unannounced assessments by DHS officials. The physical aspects associated with contractor activities shall also be subject to such assessments.

On a periodic basis, the DHS and its Components, including the DHS Office of Inspector General, may choose to evaluate any or all of the security controls implemented by the contractor under these clauses. Evaluation could include, but it not limited to vulnerability scanning. The DHS and its Components reserve the right to conduct audits at their discretion. With ten working days' notice, at the request of the Government, the contractor shall fully cooperate and facilitate in a Government-sponsored security control assessment at each location wherein DHS information is processed or stored, or information systems are developed, operated, maintained, or used on behalf of DHS, including those initiated by the Office of the Inspector General. The government may conduct a security control assessment on shorter notice (to include unannounced assessments) determined by DHS in the event of a security incident.

Enterprise Security Architecture

The contractor shall utilize and adhere to the DHS Enterprise Security Architecture to the best of its ability and to the satisfaction of the DHS COTR. Areas of consideration could include:

- 1) Use of multi-tier design (separating web, application and data base) with policy enforcement between tiers
- 2) Compliance to DHS Identity Credential Access Management (ICAM)
- 3) Security reporting to DHS central control points (i.e. the DHS Security Operations Center (SOC) and integration into DHS Security Incident Response
- 4) Integration into DHS Change Management (for example, the Infrastructure Change Control Board (ICCB) process)
- 5) Performance of activities per continuous monitoring requirements

Continuous Monitoring

The contractor shall participate in DHS' Continuous Monitoring Strategy and methods or shall provide a Continuous Monitoring capability that the DHS determines acceptable. The DHS Chief Information Security Officer (CISO) issues annual updates to its Continuous Monitoring requirements via the Annual Information Security Performance Plan. At a minimum, the contractor shall implement the following processes:

1. Asset Management
2. Vulnerability Management
3. Configuration Management
4. Malware Management
5. Log Integration

6. Security Information Event Management (SIEM) Integration
7. Patch Management
8. Providing near-real-time security status information to the DHS SOC

Specific Protections

Specific protections that shall be provided by the contractor include, but are not limited to the following:

Security Operations

The Contractor shall operate a SOC to provide the security services described below. The Contractor shall support regular reviews with the DHS Information Security Office to coordinate and synchronize the security posture of the contractor hosting facility with that of the DHS Data Centers. The SOC personnel shall provide 24x7x365 staff to monitor the network and all of its devices. The contractor staff shall also analyze the information generated by the devices for security events, respond to real-time events, correlate security device events, and perform continuous monitoring. It is recommended that the contractor staff shall also maintain a trouble ticket system in which incidents and outages are recorded. In the event of an incident, the contractor facility SOC shall adhere to the incident response plan.

Computer Incident Response Services

The Contractor shall provide Computer Incident Response Team (CIRT) services. The contractor shall adhere to the standard Incident Reporting process as determined by the Component and is defined by a DHS-specific incident response plan that adheres to DHS policy and procedure for reporting incidents. The contractor shall conduct Incident Response Exercises to ensure all personnel are familiar with the plan. The contractor shall notify the DHS SOC of any incident in accordance with the Incident Response Plan and work with DHS throughout the incident duration.

Firewall Management and Monitoring

The Contractor shall provide firewall management services that include the design, configuration, implementation, maintenance, and operation of all firewalls within the hosted DHS infrastructure in accordance with DHS architecture and security policy. The contractor shall provide all maintenance to include configuration, patching, rule maintenance (add, modify, delete), and comply with DHS' configuration management / release management requirements when changes are required. Firewalls shall operate 24x7x365. Analysis of the firewall logs shall be reported to DHS COTR in weekly status reports. If an abnormality or anomaly is identified, the contractor shall notify the appropriate DHS point of contact in accordance with the incident response plan.

Intrusion Detection Systems and Monitoring

The Contractor shall provide the design, configuration, implementation, and maintenance of the sensors and hardware that are required to support the NIDS solution. The contractor is responsible for creating and maintaining the NIDS rule sets. The NIDS solution should provide real-time alerts. These alerts and other relevant information shall be located in a central repository. The NIDS shall operate 24x7x365. A summary of alerts shall be reported to DHS COTR in weekly status reports. If an abnormality or anomaly is identified, the contractor shall notify the appropriate DHS point of contact in accordance with the incident response plan.

Physical and Information Security and Monitoring

The Contractor shall provide a facility using appropriate protective measures to provide for physical security. The facility will be located within the United States and its territories. The contractor shall maintain a process to control physical access to DHS IT assets. DHS IT Assets shall be monitored 24x7x365. A summary of unauthorized access attempts shall be reported to the appropriate DHS security office.

Vulnerability Assessments

The Contractor shall provide all information from any managed device to DHS, as requested, and shall assist, as needed, to perform periodic vulnerability assessments of the network, operating systems, and applications to identify vulnerabilities and propose mitigations. Vulnerability assessments shall be included as part of compliance with the continuous monitoring of the system.

Anti-malware (e.g., virus, spam)

The Contractor shall design, implement, monitor and manage to provide comprehensive anti-malware service. The contractor shall provide all maintenance for the system providing the anti-malware capabilities to include configuration, definition updates, and comply with DHS' configuration management / release management requirements when changes are required. A summary of alerts shall be reported to DHS COTR in weekly status reports. If an abnormality or anomaly is identified, the contractor shall notify the appropriate DHS point of contact in accordance with the incident response plan.

Patch Management

The Contractor shall perform provide patch management services. The contractor shall push patches that are required by vendors and the DHS system owner. This is to ensure that the infrastructure and applications that directly support the DHS information system are current in their release and that all

security patches are applied. The contractor shall be informed by DHS which patches that are required by DHS through the Information Security Vulnerability Management bulletins and advisories. Core applications, the ones DHS utilizes to fulfill their mission, shall be tested by DHS. However, the contractor shall be responsible for deploying patches as directed by DHS. It is recommended that all other applications (host-based intrusion detection system (HIDS), network intrusion detection system (NIDS), Anti-malware, and Firewall) shall be tested by the contractor prior to deployment in a test environment.

Log Retention

Log files for all infrastructure devices, physical access, and anti-malware should be retained online for 180 days and offline for three years.

Personal Identification Verification (PIV) Credential Compliance

Authorities:

HSPD-12 —Policies for a Common Identification Standard for Federal Employees and Contractors

OMB M-11-11 "Continued Implementation of Homeland Security Presidential Directive (HSPD) 12—Policy for a Common Identification Standard for Federal Employees and Contractors"

OMB M-06-16 —Acquisition of Products and Services for Implementation of HSPD-12

NIST FIPS 201 —Personal Identity Verification (PIV) of Federal Employees and Contractors

NIST SP 800-63 —Electronic Authentication Guidelines

OMB M-10-15 —FY 2010 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management

Procurements for products, systems, services, hardware, or software involving controlled facility or information system shall be PIV-enabled by accepting HSPD-12 PIV credentials as a method of identity verification and authentication.

Procurements for software products or software developments shall be compliant by PIV by accepting PIV credentials as the common means of authentication for access for federal employees and contractors.

PIV-enabled information systems must demonstrate that they can correctly work with PIV credentials by responding to the cryptographic challenge in the authentication protocol before granting access.

If a system is identified to be non-compliant with HSPD-12 for PIV credential enablement, a remediation plan for achieving HSPD-12 compliance shall be required for review, evaluation, and approval by the CISO.

Section 508 Requirements

Section 508 of the Rehabilitation Act, as amended by the Workforce Investment Act of 1998 (P.L. 105-220) (codified at 29 U.S.C. § 794d) requires that when Federal agencies develop, procure, maintain, or use information and communications technology (ICT), it shall be accessible to people with disabilities. Federal employees and members of the public with disabilities must be afforded access to and use of information and data comparable to that of Federal employees and members of the public without disabilities.

1. All products, platforms and services delivered as part of this work statement that, by definition, are deemed ICT or that contain ICT shall conform to the revised regulatory implementation of Section 508 Standards, which are located at 36 C.F.R. § 1194.1 & Apps. A, C & D, and available at <https://www.gpo.gov/fdsys/pkg/CFR-2017-title36-vol3/pdf/CFR-2017-title36-vol3-part1194.pdf>. In the revised regulation, ICT replaced the term electronic and information technology (EIT) used in the original 508 standards.

Item that contains Information and Communications Technology (ICT): Browsers

Applicable Exception: N/A **Authorization #:** N/A

Applicable Functional Performance Criteria: All functional performance criteria apply to when using an alternative design or technology that results to achieve substantially equivalent or greater accessibility and usability by individuals with disabilities than would be provided by conformance to one or more of the requirements in Chapters 4 and 5 of the Revised 508 Standards, or when Chapters 4 or 5 do not address one or more functions of ICT.

Applicable requirements for electronic content features and components (including Internet and Intranet website; Electronic documents; Electronic document templates; Electronic reports; Electronic training materials): All Level AA Success Criteria Apply

Applicable requirements for software features and components (including Software infrastructure): All WCAG Level AA Success Criteria, 502 Interoperability with Assistive Technology, 503 Application, 504 Authoring Tools

Applicable requirements for hardware features and components: Does not apply

Applicable support services and documentation: All requirements apply

2. When providing installation, configuration or integration services for ICT, the contractor shall not reduce the original ICT item's level of Section 508 conformance prior to the services being performed.
3. When providing maintenance upgrades, substitutions, and replacements to ICT, the contractor shall not reduce the original ICT's level of Section 508 conformance prior to upgrade, substitution or replacement. Prior to acceptance, the contractor shall provide an Accessibility Conformance Report (ACR). The ACR should be created using the on the Voluntary Product

Accessibility Template Version 2.1 or later. The template can be located at <https://www.itic.org/policy/accessibility/vpat>

4. When developing or modifying ICT for the government, the contractor shall ensure the ICT fully conforms to the applicable Section 508 Standards. When modifying a commercially available or government-owned ICT, the contractor shall not reduce the original ICT Item's level of Section 508 conformance.
5. When developing or modifying web and software ICT, the contractor shall demonstrate Section 508 conformance by providing Section 508 test results based on the versions of the DHS Trusted Tester Methodology currently approved for use, as defined at <https://www.dhs.gov/compliance-test-processes>. The contractor shall use testers who are certified by DHS on how to use the DHS Trusted Tester Methodology (e.g "DHS Certified Trusted Testers") to conduct accessibility testing. Information on how testers can become certified is located at <https://www.dhs.gov/publication/trusted-tester-resources>.
6. Exceptions for this work statement have been determined by DHS and only the exceptions described herein may be applied. Any request for additional exceptions shall be sent to the Contracting Officer and a determination will be made according to DHS Directive 139-05, Office of Accessible Systems and Technology, dated January 29, 2016 and DHS Instruction 139-05-001, Managing the Accessible Systems and Technology Program, dated January 11, 2017.
7. Where ICT conforming to one or more requirements in the Revised 508 Standards is not commercially available, the agency shall procure the ICT that best meets the Revised 508 Standards consistent with the agency's business needs, in accordance with 36 CFR E202.7. Any selection of a product or service that meets less accessibility standards due to a significant difficulty or expense shall only be permitted under an undue burden claim and requires authorization from the DHS Office of Accessible Systems and Technology (OAST) according to DHS Directive 139-05, Office of Accessible Systems and Technology, dated January 29, 2016 and DHS Instruction 139-05-001, Managing the Accessible Systems and Technology Program, dated January 11, 2017 and 36 CFR E202.6.

Instructions to Offerors

1. For each commercially available Information and Communications Technology (ICT) item offered through this contract, the Offeror shall provide an Accessibility Conformance Report (ACR). The ACR shall be created using the Voluntary Product Accessibility Template Version 2.1 or later. The template can be found at <https://www.itic.org/policy/accessibility/vpat>. Each ACR shall be completed in accordance with all the instructions provided in the VPAT 2. template. Each ACR must address the applicable Section 508 requirements referenced in the Work Statement. Each ACR shall state exactly how the ICT meets the applicable standards in the remarks/explanations column, or through additional narrative. All "Supports", "Supports with Exceptions", "Does Not Support", and "Not Applicable" (N/A) responses must be explained in the remarks/explanations column or through additional narrative. The offeror is cautioned to address each standard individually and with specificity, and to be clear whether conformance is achieved throughout the entire ICT Item (for example - user functionality, administrator functionality, and reporting), or only in limited areas of the ICT Item. The ACR shall provide a description of the evaluation methods used to support Section 508 conformance

claims. The agency reserves the right, prior to making an award decision, to perform testing on some or all of the Offeror's proposed ICT items to validate Section 508 conformance claims made in the ACR.

2. For each commercially available authoring tool offered that generates electronic content (e.g., an authoring tool that is used to create html pages, reports, surveys, charts, dashboards, etc.), the Offeror shall describe the level of Section 508 compliance supported for the content that can be generated.
3. The offeror shall provide describe accessibility remediation plans for features that don't fully conform to the Section 508 Standards.

Acceptance Criteria

1. Before accepting items that contain Information and Communications Technology (ICT) that are developed, modified, or configured according to this contract, the government reserves the right to require the contractor to provide the following:
 - o Accessibility test results based on the required test methods.
 - o Documentation of features provided to help achieve accessibility and usability for people with disabilities.
 - o Documentation of core functions that cannot be accessed by persons with disabilities.
 - o Documentation on how to configure and install the ICT Item to support accessibility.
 - o Demonstration of the ICT Item's conformance to the applicable Section 508 Standards, (including the ability of the ICT Item to create electronic content – where applicable).
2. Before accepting ICT required under the contract, the government reserves the right to perform testing on required ICT items to validate the offeror's Section 508 conformance claims. If the government determines that Section 508 conformance claims provided by the offeror represent a higher level of conformance than what is actually provided to the agency, the government shall, at its option, require the offeror to remediate the item to align with the offeror's original Section 508 conformance claims prior to acceptance.

ISO (Information Security) COMPLIANCE

- **Information Security Clause:**

"All services provided under this task order must be compliant with DHS Information Security Policy, identified in MD4300.1, *Information Technology Systems Security Program* and *4300A Sensitive Systems Handbook*."

- **Interconnection Security Agreements**

Interconnections between DHS and non-DHS IT systems shall be established only through controlled interfaces and via approved service providers. The controlled interfaces shall be accredited at the highest security level of information on the network. Connections with other Federal agencies shall be documented based on interagency agreements; memoranda of understanding, service level agreements or interconnect service agreements.

Attachment 3-

**ITEMS AND PRICES, DELIVERY SCHEDULE AND ACCOUNTING DATA
FOR
DELIVERY ORDER: 70B04C18F00001257**

I.1 SCHEDULE OF SUPPLIES/SERVICES

| ITEM # | DESCRIPTION | QTY | UNIT | UNIT PRICE | EXT. PRICE |
|--------|-------------|-------|------|------------|------------|
| 10 | (b) (7)(E) | 1.000 | EA | (b) (4) | (b) (4) |
| 20 | (b) (7)(E) | 1.000 | EA | (b) (4) | (b) (4) |

Total Funded Value of Award:

\$870,000.00

I.2 ACCOUNTING and APPROPRIATION DATA

| ITEM # | ACCOUNTING and APPROPRIATION DATA | AMOUNT |
|--------|--|-----------|
| 10 | 6100.315BUSCSGLCS0942710700Z00018500MA110000AHIB IR800315B TAS# 07020182018 0530000 | \$(b) (4) |
| 20 | 6100.315BUSCSGLCS0942710700Z00018500TT060000AHIE IU800315B TAS# 07020182018 0530000 | \$(b) (4) |

I.3 DELIVERY SCHEDULE

| DELIVER TO: | ITEM # | QTY | DELIVERY DATE |
|--|--------|-------|---------------|
| US Customs and Border Protection (b) (7)(E) | 10 | 1.000 | (b) (7)(E) |
| | 20 | 1.000 | (b) (7)(E) |

I.4 52.232-39 UNENFORCEABILITY OF UNAUTHORIZED OBLIGATIONS (JUN 2013)

(a) Except as stated in paragraph (b) of this clause, when any supply or service acquired under this contract is subject to any End User License Agreement (EULA), Terms of Service (TOS), or similar legal instrument or agreement, that includes any clause requiring the Government to indemnify the Contractor or any person or entity for damages, costs, fees, or any other loss or liability that would create an Anti-Deficiency Act violation (31 U.S.C. 1341), the following shall govern:

(1) Any such clause is unenforceable against the Government.

(2) Neither the Government nor any Government authorized end user shall be deemed to have agreed to such clause by virtue of it appearing in the EULA, TOS, or similar legal instrument or agreement. If the EULA, TOS, or similar legal instrument or agreement is invoked through an "I agree" click box or other comparable mechanism (e.g., "click-wrap" or "browse-wrap" agreements), execution does not bind the Government or any Government authorized end user to such clause.

(3) Any such clause is deemed to be stricken from the EULA, TOS, or similar legal instrument or agreement.

(b) Paragraph (a) of this clause does not apply to indemnification by the Government that is expressly authorized by statute and specifically authorized under applicable agency regulations and procedures.

(End of clause)

I.5 52.232-40 PROVIDING ACCELERATED PAYMENTS TO SMALL BUSINESS SUBCONTRACTORS (DEC 2013)

(a) Upon receipt of accelerated payments from the Government, the Contractor shall make accelerated payments to its small business subcontractors under this contract, to the maximum extent practicable and prior to when such payment is otherwise required under the applicable contract or subcontract, after receipt of a proper invoice and all other required documentation from the small business subcontractor.

(b) The acceleration of payments under this clause does not provide any new rights under the Prompt Payment Act.

- (c) Include the substance of this clause, including this paragraph (c), in all subcontracts with small business concerns, including subcontracts with small business concerns for the acquisition of commercial items.

(End of clause)

I.6 52.203-19 PROHIBITION ON REQUIRING CERTAIN INTERNAL CONFIDENTIALITY AGREEMENTS OR STATEMENTS (JAN 2017)

I.7 52.204-22 ALTERNATIVE LINE ITEM PROPOSAL (JAN 2017)

I.8 52.204-23 - PROHIBITION ON CONTRACTING FOR HARDWARE, SOFTWARE, AND SERVICES DEVELOPED OR PROVIDED BY KASPERSKY LAB AND OTHER COVERED ENTITIES (JUL 2018)

I.9 52.209-10 PROHIBITION ON CONTRACTING WITH INVERTED DOMESTIC CORPORATIONS (NOV 2015)

I.10 3052.205-70 ADVERTISEMENTS, PUBLICIZING AWARDS, AND RELEASES (SEP 2012) ALTERNATE I (SEP 2012)

- (a) The Contractor shall not refer to this contract in commercial advertising or similar promotions in such a manner as to state or imply that the product or service provided is endorsed or preferred by the Federal Government or is considered by the Government to be superior to other products or services.
- (b) All advertisements, releases, announcements, or other publication regarding this contract or the agency programs and projects covered under it, or the results or conclusions made pursuant to performance, must be approved by the Contracting Officer. Under no circumstances shall the Contractor, or anyone acting on behalf of the Contractor, refer to the supplies, services, or equipment furnished pursuant to the provisions of this contract in any publicity, release, or commercial advertising without first obtaining explicit written consent to do so from the Contracting Officer.

(End of clause)

I.11 52.224-3 PRIVACY TRAINING, ALTERNATE I (DEVIATION)

- (a) Definition. As used in this clause, personally identifiable information means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. (See Office of Management and Budget (OMB) *Circular A-130, Managing Federal Information as a Strategic Resource*).
- (b) The Contractor shall ensure that initial privacy training, and annual privacy training thereafter, is completed by contractor employees who--
- (1) Have access to a system of records;
 - (2) Create, collect, use, process, store, maintain, disseminate, disclose, dispose, or otherwise handle personally identifiable information on behalf of an agency; or
 - (3) Design, develop, maintain, or operate a system of records (see also FAR subpart 24.1 and 39.105).
- (c) The contracting agency will provide initial privacy training, and annual privacy training thereafter, to Contractor employees for the duration of this contract. Contractor employees shall satisfy this requirement by completing *Privacy at DHS: Protecting Personal Information* accessible at <http://www.dhs.gov/dhs-security-and-training-requirements-contractors>. Training shall be completed within 30 days of contract award and be completed on an annual basis thereafter not later than October 31st of each year.
- (d) The Contractor shall maintain and, upon request, provide documentation of completion of privacy training to the Contracting Officer.
- (e) The Contractor shall not allow any employee access to a system of records, or permit any employee to create, collect, use, process, store, maintain, disseminate, disclose, dispose or otherwise handle personally identifiable information, or

70B04C18F00001257

to design, develop, maintain, or operate a system of records unless the employee has completed privacy training, as required by this clause.

(f) The substance of this clause, including this paragraph (f), shall be included in all subcontracts under this contract, when subcontractor employees will –

- (1) Have a system of records;
- (2) Create, collect, use, process, store, maintain, disseminate, disclose, dispose or otherwise handle personally identifiable information; or
- (3) Design, develop, maintain, or operate a system of records.

(End of clause)

I.12 TERM OF CONTRACT (MARCH 2003)

The term of this contract is from September 25, 2018 to September 24, 2019.

[End of Clause]

I.13 CONTRACTING OFFICER'S AUTHORITY (MAR 2003)

The Contracting Officer is the only person authorized to approve changes in any of the requirements of this contract. In the event the Contractor effects any changes at the direction of any person other than the Contracting Officer, the changes will be considered to have been made without authority and no adjustment will be made in the contract price to cover any increase in costs incurred as a result thereof. The Contracting Officer shall be the only individual authorized to accept nonconforming work, waive any requirement of the contract, or to modify any term or condition of the contract. The Contracting Officer is the only individual who can legally obligate Government funds. No cost chargeable to the proposed contract can be incurred before receipt of a fully executed contract or specific authorization from the Contracting Officer.

[End of Clause]

I.14 ELECTRONIC INVOICING AND PAYMENT REQUIREMENTS - INVOICE PROCESSING PLATFORM (IPP) (JAN 2016)

Beginning April 11, 2016, payment requests for all new awards must be submitted electronically through the U. S. Department of the Treasury's Invoice Processing Platform System (IPP). Payment terms for existing contracts and orders awarded prior to April 11, 2016 remain the same. The Contractor must use IPP for contracts and orders awarded April 11, 2016 or later, and must use the non-IPP invoicing process for those contracts and orders awarded prior to April 11, 2016.

"Payment request" means any request for contract financing payment or invoice payment by the Contractor. To constitute a proper invoice, the payment request must comply with the requirements identified in FAR 32.905(b), "Payment documentation and process" and the applicable Prompt Payment clause included in this contract. The IPP website address is: <https://www.ipp.gov>.

Under this contract, the following documents are required to be submitted as an attachment to the IPP:

Copy of Invoice

- _____
- _____
- _____
- _____

The IPP was designed and developed for Contractors to enroll, access and use IPP for submitting requests for payment. Contractor assistance with enrollment can be obtained by contacting IPPCustomerSupport@fms.treas.gov or phone (866) 973-3131.

If the Contractor is unable to comply with the requirement to use IPP for submitting invoices for payment, the Contractor must submit a waiver request in writing to the contracting officer.

(End of Clause)

I.15 GOVERNMENT CONSENT OF PUBLICATION/ENDORSEMENT (MAR 2003)

Under no circumstances shall the Contractor, or anyone acting on behalf of the Contractor, refer to the supplies, services, or equipment furnished pursuant to the provisions of this contract in any news release or commercial advertising without first obtaining explicit written consent to do so from the Contracting Officer

The Contractor agrees not to refer to awards in commercial advertising in such a manner as to state or imply that the product or service provided is endorsed or preferred by the Federal Government or is considered by the Government to be superior to other products or services.

[End of Clause]

I.16 SECURITY PROCEDURES (OCT 2009)

A. Controls

1. The Contractor shall comply with the U.S. Customs and Border Protection (CBP) administrative, physical and technical security controls to ensure that the Government's security requirements are met.
2. All Government furnished information must be protected to the degree and extent required by local rules, regulations, and procedures. The Contractor shall comply with all security policies contained in CBP Handbook 1400-05C, Information Systems Security Policies and Procedures Handbook.
3. All services provided under this contract must be compliant with the Department of Homeland Security (DHS) information security policy identified in DHS Management Directive (MD) 4300.1, Information Technology Systems Security Program and DHS 4300A, Sensitive Systems Handbook.
4. All Contractor employees under this contract must wear identification access badges when working in CBP facilities. Prior to Contractor employees' departure/separation, all badges, building passes, parking permits, keys and pass cards must be given to the Contracting Officer's Technical Representative (COTR). The COTR will ensure that the cognizant Physical Security official is notified so that access to all buildings and facilities can be revoked. NOTE: For contracts within the National Capitol Region (NCR), the Office of Internal Affairs, Security Management Division (IA/SMD) should be notified if building access is revoked.
5. All Contractor employees must be registered in the Contractor Tracking System (CTS) database by the Contracting Officer (CO) or COTR. The Contractor shall provide timely start information to the CO/COTR or designated government personnel to initiate the CTS registration. Other relevant information will also be needed for registration in the CTS database such as, but not limited to, the contractor's legal name, address, brief job description, labor rate, Hash ID, schedule and contract specific information. The CO/COTR or designated government personnel shall provide the Contractor with instructions for receipt of CTS registration information. Additionally, the CO/COTR shall immediately notify IA/SMD of the contractor's departure/separation.
6. The Contractor shall provide employee departure/separation date and reason for leaving to the CO/COTR in accordance with CBP Directive 51715-006, Separation Procedures for Contractor Employees. Failure by the Contractor to provide timely notification of employee departure/separation in accordance with the contract requirements shall be documented and considered when government personnel completes a Contractor Performance Report (under Business Relations) or other performance related measures.

B. Security Background Investigation Requirements

1. In accordance with DHS Management Directive (MD) 11055, Suitability Screening Requirements for Contractors, Part VI, Policy and Procedures, Section E, Citizenship and Residency Requirements, contractor employees who require access to sensitive information must be U.S. citizens or have Lawful Permanent Resident (LPR) status. A waiver may be granted, as outlined in MD 11055, Part VI, Section M (1).
2. Contractor employees that require access to DHS IT systems or development, management, or maintenance of those systems must be U.S. citizens in accordance with MD 11055, Part VI, Section E (Lawful Permanent Resident status is not acceptable in this case). A waiver may be granted, as outlined in MD 11055, Part VI, Section M (2)

3. Provided the requirements of DHS MD 11055 are met as outlined in paragraph 1, above, contractor employees requiring access to CBP facilities, sensitive information or information technology resources are required to have a favorably adjudicated background investigation (BI) or a single scope background investigation (SSBI) prior to commencing work on this contract. Exceptions shall be approved on a case-by-case basis with the employee's access to facilities, systems, and information limited until the Contractor employee receives a favorably adjudicated BI or SSBI. A favorable adjudicated BI or SSBI shall include various aspects of a Contractor employee's life, including employment, education, residences, police and court inquiries, credit history, national agency checks, and a CBP Background Investigation Personal Interview (BIPI).
4. The Contractor shall submit within ten (10) working days after award of this contract a list containing the full name, social security number, place of birth (city and state), and date of birth of employee candidates who possess favorably adjudicated BI or SSBI that meets federal investigation standards.. For employee candidates needing a BI for this contract, the Contractor shall require the applicable employees to submit information and documentation requested by CBP to initiate the BI process.
5. Background Investigation information and documentation is usually submitted by completion of standard federal and agency forms such as Questionnaire for Public Trust and Selected Positions or Questionnaire for National Security Positions; Fingerprint Chart; Fair Credit Reporting Act (FCRA) form; Criminal History Request form; and Financial Disclosure form. These forms must be submitted to the designated CBP official identified in this contract. The designated CBP security official will review the information for completeness.
6. The estimated completion of a BI or SSBI is approximately sixty (60) to ninety (90) days from the date of receipt of the properly completed forms by CBP security office. During the term of this contract, the Contractor is required to provide the names of contractor employees who successfully complete the CBP BI or SSBI process. Failure of any contractor employee to obtain and maintain a favorably adjudicated BI or SSBI shall be cause for dismissal. For key personnel, the Contractor shall propose a qualified replacement employee candidate to the CO and COTR within 30 days after being notified of an unsuccessful candidate or vacancy. For all non-key personnel contractor employees, the Contractor shall propose a qualified replacement employee candidate to the COTR within 30 days after being notified of an unsuccessful candidate or vacancy. The CO/COTR shall approve or disapprove replacement employees. Continuous failure to provide contractor employees who meet CBP BI or SSBI requirements may be cause for termination of the contract.

C. Security Responsibilities

1. The Contractor shall ensure that its employees follow the general procedures governing physical, environmental, and information security described in the various DHS CBP regulations identified in this clause. The contractor shall ensure that its employees apply proper business practices in accordance with the specifications, directives, and manuals required for conducting work under this contract. Applicable contractor personnel will be responsible for physical security of work areas and CBP furnished equipment issued under this contract.
2. The CO/COTR may require the Contractor to prohibit its employees from working on this contract if continued employment becomes detrimental to the public's interest for any reason including, but not limited to carelessness, insubordination, incompetence, or security concerns.
3. Work under this contract may require access to sensitive information as defined under Homeland Security Acquisition Regulation (HSAR) Clause 3052.204-71, Contractor Employee Access, included in the solicitation/contract. The Contractor shall not disclose, orally or in writing, any sensitive information to any person unless authorized in writing by the CO.
4. The Contractor shall ensure that its employees who are authorized access to sensitive information, receive training pertaining to protection and disclosure of sensitive information. The training shall be conducted during and after contract performance.
5. Upon completion of this contract, the Contractor shall return all sensitive information used in the performance of the contract to the CO/COTR. The Contractor shall certify, in writing, that all sensitive and non-public information has been purged from any Contractor-owned system.

D. Notification of Contractor Employee Changes

1. The Contractor shall notify the CO/COTR via phone, facsimile, or electronic transmission, immediately after a personnel change become known or no later than five (5) business days prior to departure of the employee. Telephone notifications must be immediately followed up in writing. Contractor's notification shall include, but is not limited to name changes, resignations, terminations, and reassignments to another contract.
2. The Contractor shall notify the CO/COTR and program office (if applicable) in writing of any proposed change in access requirements for its employees at least fifteen (15) days, or thirty (30) days if a security clearance is to be obtained, in advance of the proposed change. The CO/COTR will notify the Office of Information and Technology (OIT) Information Systems Security Branch (ISSB) of the proposed change. If a security clearance is required, the CO/COTR will notify IA/SMD.

E. Non-Disclosure Agreements

When determined to be appropriate, Contractor employees are required to execute a non-disclosure agreement (DHS Form 11000-6) as a condition to access sensitive but unclassified information.

[End of Clause]

I.17 SPECIAL SECURITY REQUIREMENT - CONTRACTOR PRE-SCREENING (SEP 2011)

1. Contractors requiring recurring access to Government facilities or access to sensitive but unclassified information and/or logical access to Information Technology (IT) resources shall verify minimal fitness requirements for all persons/candidates designated for employment under any Department of Security (DHS) contract by pre-screening the person /candidate prior to submitting the name for consideration to work on the contract. Pre-screening the candidate ensures that minimum fitness requirements are considered and mitigates the burden of DHS having to conduct background investigations on objectionable candidates. The Contractor shall submit only those candidates that have not had a felony conviction within the past 36 months or illegal drug use within the past 12 months from the date of submission of their name as a candidate to perform work under this contract. Contractors are required to flow this requirement down to subcontractors. Pre-screening involves contractors and subcontractors reviewing:
 - a. Felony convictions within the past 36 months. An acceptable means of obtaining information on felony convictions is from public records, free of charge, or from the National Crime Information Center (NCIC).
 - b. Illegal drug use within the past 12 months. An acceptable means of obtaining information related to drug use is through employee self certification, by public records check; or if the contractor or subcontractor already has drug testing in place. There is no requirement for contractors and/or subcontractors to initiate a drug testing program if they do not have one already in place.
 - c. Misconduct such as criminal activity on the job relating to fraud or theft within the past 12 months. An acceptable means of obtaining information related to misconduct is through employee self certification, by public records check, or other reference checks conducted in the normal course of business.
2. Pre-screening shall be conducted within 15 business days after contract award. This requirement shall be placed in all subcontracts if the subcontractor requires routine physical access, access to sensitive but unclassified information, and/or logical access to IT resources. Failure to comply with the pre-screening requirement will result in the Contracting Officer taking the appropriate remedy.

Definition: *Logical Access* means providing an authorized user the ability to access one or more computer system resources such as a workstation, network, application, or database through automated tools. A logical access control system (LACS) requires validation of an individual identity through some mechanism such as a personal identification number (PIN), card, username and password, biometric, or other token. The system has the capability to assign different access privileges to different persons depending on their roles and responsibilities in an organization.

[End of Clause]

ORDER FOR SUPPLIES OR SERVICES

PAGE OF PAGES

1 2

IMPORTANT: Mark all packages and papers with contract and/or order numbers.

| | | | | |
|---|--|--|----------|-------------|
| 1. DATE OF ORDER 09/25/2018 | 2. CONTRACT NO. (if any) HSHQDC13D00027 | 6. SHIP TO: | | |
| 3. ORDER NO. 70B04C18F00001257 | | 4. REQUISITION/REFERENCE NO. 0020098303 | | |
| 5. ISSUING OFFICE (Address correspondence to) DHS - Customs & Border Protection Department of Homeland Security 1300 Pennsylvania Avenue, NW NP 1310 Washington DC 20229 | | a. NAME OF CONSIGNEE See Attached Delivery Schedule | | |
| | | b. STREET ADDRESS | | |
| | | c. CITY | d. STATE | e. ZIP CODE |
| | | f. SHIP VIA | | |

| | | | | |
|---|--|---|--|--|
| 7. TO: | | 8. TYPE OF ORDER | | |
| a. NAME OF CONTRACTOR TROFHOLZ TECHNOLOGIES, INC | | <input type="checkbox"/> a. PURCHASE -- Reference Your . Please furnish the following on the terms and conditions specified on both sides of this order and on the attached sheet, if any, including delivery as indicated. | <input checked="" type="checkbox"/> b. DELIVERY -- Except for billing instructions on the reverse, this delivery order is subject to instructions contained on this side only of this form and is issued subject to the terms and conditions of the above-numbered contract. | |
| b. COMPANY NAME | | | | |
| c. STREET ADDRESS 2207 PLAZA DRIVE, STE 100 | | | | |

| | | | | |
|---|----------------|---------------------------|--|--|
| d. CITY ROCKLIN | e. STATE CA | f. ZIP CODE 95765-4415 | 10. REQUISITIONING OFFICE (b) (7)(E), (b) (6), (b) (7)(C) | |
| 9. ACCOUNTING AND APPROPRIATION DATA SEE ACCOUNTING & APPROP. DATA SHEET | | | | |

| | | | | | |
|--|---|---|--|-------------------------------------|----------------|
| 11. BUSINESS CLASSIFICATION (Check appropriate box(es)) | | | | 12. F.O.B. POINT | |
| <input checked="" type="checkbox"/> a. SMALL | <input type="checkbox"/> b. OTHER THAN SMALL | <input type="checkbox"/> c. DISADVANTAGED | <input type="checkbox"/> d. WOMEN-OWNED | <input type="checkbox"/> e. HUBZone | |
| <input type="checkbox"/> f. SERVICE-DISABLED VETERAN-OWNED | <input type="checkbox"/> g. WOMEN-OWNED SMALL BUSINESS (WOSB) ELIGIBLE UNDER THE WOSB PROGRAM | | <input type="checkbox"/> h. ECONOMICALLY DISADVANTAGED WOMEN-OWNED SMALL BUSINESS (EDWOSB) | | Not applicable |

| | | | | |
|---------------|---------------|------------------------|--|--|
| 13. PLACE OF | | 14. GOVERNMENT B/L NO. | 15. DELIVER TO F.O.B POINT ON OR BEFORE (Date) 09/24/2019 | 16. DISCOUNT TERMS Within 30 days Due net |
| a. INSPECTION | b. ACCEPTANCE | | | |

| 17. SCHEDULE (See reverse for Rejections) | | | | | | |
|---|--------------------------|----------------------|----------|----------------|------------|------|
| ITEM NO. (a) | SUPPLIES OR SERVICES (b) | QUANTITY ORDERED (c) | UNIT (d) | UNIT PRICE (e) | AMOUNT (f) | Acpt |
| 10 | (b) (7)(E) | 1.000 | EA | (b) (4) | | |
| 20 | (b) (7)(E) | 1.000 | EA | | | |

| | | | |
|--|---------------------------|---------------------------|--------------------------|
| 18. SHIPPING POINT | 19. GROSS SHIPPING WEIGHT | 20. INVOICE NO. | 17(h) TOT. (Cont. pages) |
| 21. MAIL INVOICE TO: | | | |
| a. NAME DHS - Customs & Border Protection | | Commercial Accounts Sect. | \$0.00 |
| b. STREET ADDRESS (or P.O. Box) 6650 Telecom Drive, Suite 100 | | | 17(i) GRAND TOTAL |
| c. CITY Indianapolis | d. STATE IN | e. ZIP CODE 46278 | |

| | | | |
|---|---------------------|---|-------------------------------------|
| 22. UNITED STATES OF AMERICA BY (Signature) | (b) (6), (b) (7)(C) | 23. NAME (Typed) (b) (6), (b) (7)(C) | TITLE: CONTRACTING/ORDERING OFFICER |
|---|---------------------|---|-------------------------------------|

AUTHORIZED FOR LOCAL REPRODUCTION
PREVIOUS EDITION NOT USABLE

| | | | |
|-----------------------------|---|--------------------------------|----------------------|
| DATE OF ORDER 09/25/2018 | CONTRACT NO. (if any) HSHQDC13D00027 | ORDER NO. 70B04C18F00001257 | PAGE OF PAGES 2 2 |
|-----------------------------|---|--------------------------------|----------------------|

Federal Tax Exempt ID

(b) (3) (A)

Emailing Invoices to CBP. Do not mail or email invoices to CBP. Invoices must be submitted via the IPP website, as detailed under Electronic Invoicing and Payment Requirements in the attached terms and conditions.

NOTES:

This Firm Fixed Price (FFP) Task Order, 70B04C18F00001257 is awarded to Trofholz Technologies, for the SILO software and maintenance, per the attached Attachment 1- Statement of Work (SOW) and Attachment 2- Bill of Materials (BOM).

The delivery of the order must be made within 30 days after the award and with a 12 month Period of Performance (POP) after award for maintenance, from

(b) (7)(E)

The total order is in the amount of \$870,000.00.

CLINS 10 and 20 are funded under the order. Attachment 3- Accounting and Appropriation Data Sheet.

The Contracting Officer (CO) (b) (6), (b) (7)(C) @cbp.dhs.gov

The Contracting Officer Representative (COR) (b) (6), (b) (7)(C) @cbp.dhs.gov

Invoicing- The IPP Invoice Platform- per section I.14 of the Accounting & Appropriation section, must be used for the invoicing after the delivery is received and accepted by CBP.

The Terms and Conditions under the DHS Award HSHQDC-13-D-00027 apply to this Task Order.

Acceptance of the order by:

(b) (6), (b) (7)(C)

**ITEMS AND PRICES, DELIVERY SCHEDULE AND ACCOUNTING DATA
 FOR
 DELIVERY ORDER: 70B04C18F00000377**

I.1 SCHEDULE OF SUPPLIES/SERVICES

| ITEM # | DESCRIPTION | QTY | UNIT | UNIT PRICE | EXT. PRICE |
|--------|-------------|-------|------|------------|------------|
| 10 | (b) (7)(E) | 1.000 | EA | (b) (4) | (b) (4) |

Total Funded Value of Award: \$508,841.42

I.2 ACCOUNTING and APPROPRIATION DATA

| ITEM # | ACCOUNTING and APPROPRIATION DATA | AMOUNT |
|--------|--|--------------|
| 10 | 6100.315BUSCSGLCS0942715000Z00018500TT0600000000 IU549315B TAS# 07020182018 0530000 | \$508,841.42 |

I.3 DELIVERY SCHEDULE

| DELIVER TO: | ITEM # | QTY | DELIVERY DATE |
|--|--------|-------|---------------|
| Customs and Border Protection (b) (6), (b) (7)(C) (b) (7)(E) Tel. #: (b) (6), (b) (7)(C) Fax #: (b) (6), (b) (7)(C) Email: (b) (6), (b) (7)(C) @cbp.dhs.gov | 10 | 1.000 | (b) (7)(E) |

I.4 52.232-39 UNENFORCEABILITY OF UNAUTHORIZED OBLIGATIONS (JUN 2013)

(a) Except as stated in paragraph (b) of this clause, when any supply or service acquired under this contract is subject to any End User License Agreement (EULA), Terms of Service (TOS), or similar legal instrument or agreement, that includes any clause requiring the Government to indemnify the Contractor or any person or entity for damages, costs, fees, or any other loss or liability that would create an Anti-Deficiency Act violation (31 U.S.C. 1341), the following shall govern:

- (1) Any such clause is unenforceable against the Government.
- (2) Neither the Government nor any Government authorized end user shall be deemed to have agreed to such clause by virtue of it appearing in the EULA, TOS, or similar legal instrument or agreement. If the EULA, TOS, or similar legal instrument or agreement is invoked through an "I agree" click box or other comparable mechanism (e.g., "click-wrap" or "browse-wrap" agreements), execution does not bind the Government or any Government authorized end user to such clause.
- (3) Any such clause is deemed to be stricken from the EULA, TOS, or similar legal instrument or agreement.

(b) Paragraph (a) of this clause does not apply to indemnification by the Government that is expressly authorized by statute and specifically authorized under applicable agency regulations and procedures.

(End of clause)

I.5 52.232-40 PROVIDING ACCELERATED PAYMENTS TO SMALL BUSINESS SUBCONTRACTORS (DEC 2013)

(a) Upon receipt of accelerated payments from the Government, the Contractor shall make accelerated payments to its small business subcontractors under this contract, to the maximum extent practicable and prior to when such payment

is otherwise required under the applicable contract or subcontract, after receipt of a proper invoice and all other required documentation from the small business subcontractor.

- (b) The acceleration of payments under this clause does not provide any new rights under the Prompt Payment Act.
- (c) Include the substance of this clause, including this paragraph (c), in all subcontracts with small business concerns, including subcontracts with small business concerns for the acquisition of commercial items.

(End of clause)

I.6 52.203-19 PROHIBITION ON REQUIRING CERTAIN INTERNAL CONFIDENTIALITY AGREEMENTS OR STATEMENTS (JAN 2017)

I.7 52.204-22 ALTERNATIVE LINE ITEM PROPOSAL (JAN 2017)

I.8 3052.205-70 ADVERTISEMENTS, PUBLICIZING AWARDS, AND RELEASES (SEP 2012) ALTERNATE I (SEP 2012)

- (a) The Contractor shall not refer to this contract in commercial advertising or similar promotions in such a manner as to state or imply that the product or service provided is endorsed or preferred by the Federal Government or is considered by the Government to be superior to other products or services.
- (b) All advertisements, releases, announcements, or other publication regarding this contract or the agency programs and projects covered under it, or the results or conclusions made pursuant to performance, must be approved by the Contracting Officer. Under no circumstances shall the Contractor, or anyone acting on behalf of the Contractor, refer to the supplies, services, or equipment furnished pursuant to the provisions of this contract in any publicity, release, or commercial advertising without first obtaining explicit written consent to do so from the Contracting Officer.

(End of clause)

I.9 3052.212-70 CONTRACT TERMS AND CONDITIONS APPLICABLE TO DHS ACQUISITION OF COMMERCIAL ITEMS (SEP 2012)

The Contractor agrees to comply with any provision or clause that is incorporated herein by reference to implement agency policy applicable to acquisition of commercial items or components. The provision or clause in effect based on the applicable regulation cited on the date the solicitation is issued applies unless otherwise stated herein. The following provisions and clauses are incorporated by reference:

[The Contracting Officer should either check the provisions and clauses that apply or delete the provisions and clauses that do not apply from the list. The Contracting Officer may add the date of the provision or clause if desired for clarity.]

(a) *Provisions.*

- 3052.209-72 Organizational Conflicts of Interest.
- 3052.216-70 Evaluation of Offers Subject to An Economic Price Adjustment Clause.
- 3052.219-72 Evaluation of Prime Contractor Participation in the DHS Mentor Protégé Program.

(b) *Clauses.*

- 3052.203-70 Instructions for Contractor Disclosure of Violations.
- 3052.204-70 Security Requirements for Unclassified Information Technology Resources.
- 3052.204-71 Contractor Employee Access.
- Alternate I
- 3052.205-70 Advertisement, Publicizing Awards, and Releases.

- 3052.209-73 Limitation on Future Contracting.
- 3052.215-70 Key Personnel or Facilities.
- 3052.216-71 Determination of Award Fee.
- 3052.216-72 Performance Evaluation Plan.
- 3052.216-73 Distribution of Award Fee.
- 3052.219-70 Small Business Subcontracting Plan Reporting.
- 3052.219-71 DHS Mentor Protégé Program.
- 3052.228-70 Insurance.
- 3052.236-70 Special Provisions for Work at Operating Airports.
- 3052.242-72 Contracting Officer's Technical Representative.
- 3052.247-70 F.o.B. Origin Information.
- Alternate I
- Alternate II
- 3052.247-71 F.o.B. Origin Only.
- 3052.247-72 F.o.B. Destination Only.

(End of clause)

I.10 52.224-3 PRIVACY TRAINING, ALTERNATE I (DEVIATION)

- (a) Definition. As used in this clause, personally identifiable information means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. (See Office of Management and Budget (OMB) *Circular A-130, Managing Federal Information as a Strategic Resource*).
- (b) The Contractor shall ensure that initial privacy training, and annual privacy training thereafter, is completed by contractor employees who--
 - (1) Have access to a system of records;
 - (2) Create, collect, use, process, store, maintain, disseminate, disclose, dispose, or otherwise handle personally identifiable information on behalf of an agency; or
 - (3) Design, develop, maintain, or operate a system of records (see also FAR subpart 24.1 and 39.105).
- (c) The contracting agency will provide initial privacy training, and annual privacy training thereafter, to Contractor employees for the duration of this contract. Contractor employees shall satisfy this requirement by completing *Privacy at DHS: Protecting Personal Information* accessible at <http://www.dhs.gov/dhs-security-and-training-requirements-contractors>. Training shall be completed within 30 days of contract award and be completed on an annual basis thereafter not later than October 31st of each year.
- (d) The Contractor shall maintain and, upon request, provide documentation of completion of privacy training to the Contracting Officer.
- (e) The Contractor shall not allow any employee access to a system of records, or permit any employee to create, collect, use, process, store, maintain, disseminate, disclose, dispose or otherwise handle personally identifiable information, or

to design, develop, maintain, or operate a system of records unless the employee has completed privacy training, as required by this clause.

(f) The substance of this clause, including this paragraph (f), shall be included in all subcontracts under this contract, when subcontractor employees will –

- (1) Have a system of records;
- (2) Create, collect, use, process, store, maintain, disseminate, disclose, dispose or otherwise handle personally identifiable information; or
- (3) Design, develop, maintain, or operate a system of records.

(End of clause)

I.11 PERIOD OF PERFORMANCE (MAR 2003)

The period of performance of this contract shall be from 06/1/2018 through 05/31/2019. However, all software licenses shall be delivered upon award.

[End of Clause]

I.12 CONTRACTING OFFICER'S AUTHORITY (MAR 2003)

The Contracting Officer is the only person authorized to approve changes in any of the requirements of this contract. In the event the Contractor effects any changes at the direction of any person other than the Contracting Officer, the changes will be considered to have been made without authority and no adjustment will be made in the contract price to cover any increase in costs incurred as a result thereof. The Contracting Officer shall be the only individual authorized to accept nonconforming work, waive any requirement of the contract, or to modify any term or condition of the contract. The Contracting Officer is the only individual who can legally obligate Government funds. No cost chargeable to the proposed contract can be incurred before receipt of a fully executed contract or specific authorization from the Contracting Officer.

[End of Clause]

I.13 ELECTRONIC INVOICING AND PAYMENT REQUIREMENTS - INVOICE PROCESSING PLATFORM (IPP) (JAN 2016)

Beginning April 11, 2016, payment requests for all new awards must be submitted electronically through the U. S. Department of the Treasury's Invoice Processing Platform System (IPP). Payment terms for existing contracts and orders awarded prior to April 11, 2016 remain the same. The Contractor must use IPP for contracts and orders awarded April 11, 2016 or later, and must use the non-IPP invoicing process for those contracts and orders awarded prior to April 11, 2016.

"Payment request" means any request for contract financing payment or invoice payment by the Contractor. To constitute a proper invoice, the payment request must comply with the requirements identified in FAR 32.905(b), "Payment documentation and process" and the applicable Prompt Payment clause included in this contract. The IPP website address is: <https://www.ipp.gov>.

Under this contract, the following documents are required to be submitted as an attachment to the IPP:

- FAR Part 32.905

The IPP was designed and developed for Contractors to enroll, access and use IPP for submitting requests for payment. Contractor assistance with enrollment can be obtained by contacting IPPCustomerSupport@fms.treas.gov or phone (866) 973-3131.

If the Contractor is unable to comply with the requirement to use IPP for submitting invoices for payment, the Contractor must submit a waiver request in writing to the contracting officer.

(End of Clause)

I.14 GOVERNMENT CONSENT OF PUBLICATION/ENDORSEMENT (MAR 2003)

Under no circumstances shall the Contractor, or anyone acting on behalf of the Contractor, refer to the supplies, services, or equipment furnished pursuant to the provisions of this contract in any news release or commercial advertising without first obtaining explicit written consent to do so from the Contracting Officer

The Contractor agrees not to refer to awards in commercial advertising in such a manner as to state or imply that the product or service provided is endorsed or preferred by the Federal Government or is considered by the Government to be superior to other products or services.

[End of Clause]

I.15 SECURITY PROCEDURES (OCT 2009)

A. Controls

1. The Contractor shall comply with the U.S. Customs and Border Protection (CBP) administrative, physical and technical security controls to ensure that the Government's security requirements are met.
2. All Government furnished information must be protected to the degree and extent required by local rules, regulations, and procedures. The Contractor shall comply with all security policies contained in CBP Handbook 1400-05C, Information Systems Security Policies and Procedures Handbook.
3. All services provided under this contract must be compliant with the Department of Homeland Security (DHS) information security policy identified in DHS Management Directive (MD) 4300.1, Information Technology Systems Security Program and DHS 4300A, Sensitive Systems Handbook.
4. All Contractor employees under this contract must wear identification access badges when working in CBP facilities. Prior to Contractor employees' departure/separation, all badges, building passes, parking permits, keys and pass cards must be given to the Contracting Officer's Technical Representative (COTR). The COTR will ensure that the cognizant Physical Security official is notified so that access to all buildings and facilities can be revoked. NOTE: For contracts within the National Capitol Region (NCR), the Office of Internal Affairs, Security Management Division (IA/SMD) should be notified if building access is revoked.
5. All Contractor employees must be registered in the Contractor Tracking System (CTS) database by the Contracting Officer (CO) or COTR. The Contractor shall provide timely start information to the CO/COTR or designated government personnel to initiate the CTS registration. Other relevant information will also be needed for registration in the CTS database such as, but not limited to, the contractor's legal name, address, brief job description, labor rate, Hash ID, schedule and contract specific information. The CO/COTR or designated government personnel shall provide the Contractor with instructions for receipt of CTS registration information. Additionally, the CO/COTR shall immediately notify IA/SMD of the contractor's departure/separation.
6. The Contractor shall provide employee departure/separation date and reason for leaving to the CO/COTR in accordance with CBP Directive 51715-006, Separation Procedures for Contractor Employees. Failure by the Contractor to provide timely notification of employee departure/separation in accordance with the contract requirements shall be documented and considered when government personnel completes a Contractor Performance Report (under Business Relations) or other performance related measures.

B. Security Background Investigation Requirements

1. In accordance with DHS Management Directive (MD) 11055, Suitability Screening Requirements for Contractors, Part VI, Policy and Procedures, Section E, Citizenship and Residency Requirements, contractor employees who require access to sensitive information must be U.S. citizens or have Lawful Permanent Resident (LPR) status. A waiver may be granted, as outlined in MD 11055, Part VI, Section M (1).
2. Contractor employees that require access to DHS IT systems or development, management, or maintenance of those systems must be U.S. citizens in accordance with MD 11055, Part VI, Section E (Lawful Permanent Resident status is not acceptable in this case). A waiver may be granted, as outlined in MD 11055, Part VI, Section M (2)
3. Provided the requirements of DHS MD 11055 are met as outlined in paragraph 1, above, contractor employees requiring access to CBP facilities, sensitive information or information technology resources are required to have a favorably adjudicated background investigation (BI) or a single scope background investigation (SSBI) prior to commencing work on this contract. Exceptions shall be approved on a case-by-case basis with the employee's

access to facilities, systems, and information limited until the Contractor employee receives a favorably adjudicated BI or SSBI. A favorable adjudicated BI or SSBI shall include various aspects of a Contractor employee's life, including employment, education, residences, police and court inquires, credit history, national agency checks, and a CBP Background Investigation Personal Interview (BIPI).

4. The Contractor shall submit within ten (10) working days after award of this contract a list containing the full name, social security number, place of birth (city and state), and date of birth of employee candidates who possess favorably adjudicated BI or SSBI that meets federal investigation standards. For employee candidates needing a BI for this contract, the Contractor shall require the applicable employees to submit information and documentation requested by CBP to initiate the BI process.
5. Background Investigation information and documentation is usually submitted by completion of standard federal and agency forms such as Questionnaire for Public Trust and Selected Positions or Questionnaire for National Security Positions; Fingerprint Chart; Fair Credit Reporting Act (FCRA) form; Criminal History Request form; and Financial Disclosure form. These forms must be submitted to the designated CBP official identified in this contract. The designated CBP security official will review the information for completeness.
6. The estimated completion of a BI or SSBI is approximately sixty (60) to ninety (90) days from the date of receipt of the properly completed forms by CBP security office. During the term of this contract, the Contractor is required to provide the names of contractor employees who successfully complete the CBP BI or SSBI process. Failure of any contractor employee to obtain and maintain a favorably adjudicated BI or SSBI shall be cause for dismissal. For key personnel, the Contractor shall propose a qualified replacement employee candidate to the CO and COTR within 30 days after being notified of an unsuccessful candidate or vacancy. For all non-key personnel contractor employees, the Contractor shall propose a qualified replacement employee candidate to the COTR within 30 days after being notified of an unsuccessful candidate or vacancy. The CO/COTR shall approve or disapprove replacement employees. Continuous failure to provide contractor employees who meet CBP BI or SSBI requirements may be cause for termination of the contract.

C. Security Responsibilities

1. The Contractor shall ensure that its employees follow the general procedures governing physical, environmental, and information security described in the various DHS CBP regulations identified in this clause. The contractor shall ensure that its employees apply proper business practices in accordance with the specifications, directives, and manuals required for conducting work under this contract. Applicable contractor personnel will be responsible for physical security of work areas and CBP furnished equipment issued under this contract.
2. The CO/COTR may require the Contractor to prohibit its employees from working on this contract if continued employment becomes detrimental to the public's interest for any reason including, but not limited to carelessness, insubordination, incompetence, or security concerns.
3. Work under this contract may require access to sensitive information as defined under Homeland Security Acquisition Regulation (HSAR) Clause 3052.204-71, Contractor Employee Access, included in the solicitation/contract. The Contractor shall not disclose, orally or in writing, any sensitive information to any person unless authorized in writing by the CO.
4. The Contractor shall ensure that its employees who are authorized access to sensitive information, receive training pertaining to protection and disclosure of sensitive information. The training shall be conducted during and after contract performance.
5. Upon completion of this contract, the Contractor shall return all sensitive information used in the performance of the contract to the CO/COTR. The Contractor shall certify, in writing, that all sensitive and non-public information has been purged from any Contractor-owned system.

D. Notification of Contractor Employee Changes

1. The Contractor shall notify the CO/COTR via phone, facsimile, or electronic transmission, immediately after a personnel change become known or no later than five (5) business days prior to departure of the employee. Telephone notifications must be immediately followed up in writing. Contractor's notification shall include, but is not limited to name changes, resignations, terminations, and reassignments to another contract.

2. The Contractor shall notify the CO/COTR and program office (if applicable) in writing of any proposed change in access requirements for its employees at least fifteen (15) days, or thirty (30) days if a security clearance is to be obtained, in advance of the proposed change. The CO/COTR will notify the Office of Information and Technology (OIT) Information Systems Security Branch (ISSB) of the proposed change. If a security clearance is required, the CO/COTR will notify IA/SMD.

E. Non-Disclosure Agreements

When determined to be appropriate, Contractor employees are required to execute a non-disclosure agreement (DHS Form 11000-6) as a condition to access sensitive but unclassified information.

[End of Clause]

I.16 SPECIAL SECURITY REQUIREMENT - CONTRACTOR PRE-SCREENING (SEP 2011)

1. Contractors requiring recurring access to Government facilities or access to sensitive but unclassified information and/or logical access to Information Technology (IT) resources shall verify minimal fitness requirements for all persons/candidates designated for employment under any Department of Security (DHS) contract by pre-screening the person /candidate prior to submitting the name for consideration to work on the contract. Pre-screening the candidate ensures that minimum fitness requirements are considered and mitigates the burden of DHS having to conduct background investigations on objectionable candidates. The Contractor shall submit only those candidates that have not had a felony conviction within the past 36 months or illegal drug use within the past 12 months from the date of submission of their name as a candidate to perform work under this contract. Contractors are required to flow this requirement down to subcontractors. Pre-screening involves contractors and subcontractors reviewing:
 - a. Felony convictions within the past 36 months. An acceptable means of obtaining information on felony convictions is from public records, free of charge, or from the National Crime Information Center (NCIC).
 - b. Illegal drug use within the past 12 months. An acceptable means of obtaining information related to drug use is through employee self certification, by public records check; or if the contractor or subcontractor already has drug testing in place. There is no requirement for contractors and/or subcontractors to initiate a drug testing program if they do not have one already in place.
 - c. Misconduct such as criminal activity on the job relating to fraud or theft within the past 12 months. An acceptable means of obtaining information related to misconduct is through employee self certification, by public records check, or other reference checks conducted in the normal course of business.
2. Pre-screening shall be conducted within 15 business days after contract award. This requirement shall be placed in all subcontracts if the subcontractor requires routine physical access, access to sensitive but unclassified information, and/or logical access to IT resources. Failure to comply with the pre-screening requirement will result in the Contracting Officer taking the appropriate remedy.

Definition: *Logical Access* means providing an authorized user the ability to access one or more computer system resources such as a workstation, network, application, or database through automated tools. A logical access control system (LACS) requires validation of an individual identity through some mechanism such as a personal identification number (PIN), card, username and password, biometric, or other token. The system has the capability to assign different access privileges to different persons depending on their roles and responsibilities in an organization.

[End of Clause]

ORDER FOR SUPPLIES OR SERVICES

PAGE OF PAGES

1 8

IMPORTANT: Mark all packages and papers with contract and/or order numbers.

| | | | | |
|--|---|--|----------|-------------|
| 1. DATE OF ORDER 09/21/2017 | 2. CONTRACT NO. (if any) HSHQDC-13-D-00026 | 6. SHIP TO: | | |
| 3. ORDER NO. HSBP1017J00831 | 4. REQUISITION/REFERENCE NO. 0020094963 | a. NAME OF CONSIGNEE See Attached Delivery Schedule | | |
| 5. ISSUING OFFICE (Address correspondence to) DHS - Customs & Border Protection Customs and Border Protection 1300 Pennsylvania Ave, NW Procurement Directorate - NP 1310 Washington DC 20229 | | b. STREET ADDRESS | | |
| | | c. CITY | d. STATE | e. ZIP CODE |
| 7. TO: | | f. SHIP VIA | | |

| | |
|--|--|
| 8. TYPE OF ORDER | |
| <input type="checkbox"/> a. PURCHASE -- Reference Your _____, Please furnish the following on the terms and conditions specified on both sides of this order and on the attached sheet, if any, including delivery as indicated. | <input checked="" type="checkbox"/> b. DELIVERY -- Except for billing instructions on the reverse, this delivery order is subject to instructions contained on this side only of this form and is issued subject to the terms and conditions of the above-numbered contract. |

| | | | |
|--|----------------|--|--|
| a. NAME OF CONTRACTOR THUNDERCAT TECHNOLOGY LLC | | 10. REQUISITIONING OFFICE (b) (6), (b) (7)(C) | |
| b. COMPANY NAME | | | |
| c. STREET ADDRESS 1925 ISAAC NEWTON SQ STE 180 | | | |
| d. CITY RESTON | e. STATE VA | f. ZIP CODE 20190-5030 | |
| 9. ACCOUNTING AND APPROPRIATION DATA SEE ATTACHED | | | |

| | | | | | |
|--|---|--|---|-------------------------------------|------------------|
| 11. BUSINESS CLASSIFICATION (Check appropriate box(es)) | | | | | 12. F.O.B. POINT |
| <input checked="" type="checkbox"/> a. SMALL | <input type="checkbox"/> b. OTHER THAN SMALL | <input type="checkbox"/> c. DISADVANTAGED | <input type="checkbox"/> d. WOMEN-OWNED | <input type="checkbox"/> e. HUBZone | Not applicable |
| <input type="checkbox"/> f. SERVICE-DISABLED VETERAN-OWNED | <input type="checkbox"/> g. WOMEN-OWNED SMALL BUSINESS (WOSB) ELIGIBLE UNDER THE WOSB PROGRAM | <input type="checkbox"/> h. ECONOMICALLY DISADVANTAGED WOMEN-OWNED SMALL BUSINESS (EDWOSB) | | | |

| | | | | |
|---------------|---------------|------------------------|--|--|
| 13. PLACE OF | | 14. GOVERNMENT B/L NO. | 15. DELIVER TO F.O.B POINT ON OR BEFORE (Date) 09/20/2018 | 16. DISCOUNT TERMS Within 30 days Due net |
| a. INSPECTION | b. ACCEPTANCE | | | |

| 17. SCHEDULE (See reverse for Rejections) | | | | | | |
|---|--------------------------|----------------------|----------|----------------|------------|------|
| ITEM NO. (a) | SUPPLIES OR SERVICES (b) | QUANTITY ORDERED (c) | UNIT (d) | UNIT PRICE (e) | AMOUNT (f) | Acpt |
| 10 | (b) (7)(E) | (b) (7)(E) | EA | (b) (4) | | |
| 20 | | | EA | | | |
| 30 | | | EA | | | |

| | | | |
|--|---------------------------|-------------------------------|--------------------------|
| 18. SHIPPING POINT | 19. GROSS SHIPPING WEIGHT | 20. INVOICE NO. | 17(h) TOT. (Cont. pages) |
| 21. MAIL INVOICE TO: | | | |
| a. NAME DHS - Customs & Border Protection | | Commercial Accounts Sect. | \$0.00 |
| b. STREET ADDRESS (or P.O. Box) | | 6650 Telecom Drive, Suite 100 | 17(i) GRAND TOTAL |
| c. CITY Indianapolis | d. STATE IN | e. ZIP CODE 46278 | |

22. UNITED STATES OF AMERICA BY (Signature) **(b) (6), (b) (7)(C)** CONTRACTING/ORDERING OFFICER

AUTHORIZED FOR LOCAL REPRODUCTION
PREVIOUS EDITION NOT USABLE

CBP
Date: 2017.09.19 14:53:43 -04'00'

OPTIONAL FORM 347 (REV. 2/2012)
Prescribed by GSA/FAR 48 CFR 53.213 (f)
USCBP000242

| | | | |
|-----------------------------|--|-----------------------------|-------------------------|
| DATE OF ORDER 09/21/2017 | CONTRACT NO. (if any) HSHQDC-13-D-00026 | ORDER NO. HSBP1017J00831 | PAGE OF PAGES 2 OF 8 |
|-----------------------------|--|-----------------------------|-------------------------|

Federal Tax Exempt ID: (b) (3) (A)

Emailing Invoices to CBP. Do not mail or email invoices to CBP. Invoices must be submitted via the IPP website, as detailed under Electronic Invoicing and Payment Requirements in the attached terms and conditions.

NOTES:

This firm-fixed-price delivery order, HSBP1017J00831, is issued against the DHS FirstSource II IDIQ Contract, HSHQDC-13-D-00026, for (b) (7)(E). The Statement of Work (SOW) has been incorporated by reference in this delivery order.

Reference: THUNDERCAT TECHNOLOGY, LLC [DUNS: 809887164] bid # 563137874 on 09/13/2017, in response to FedBid Buy # 880787_01

Delivery: The delivery of all products described in the SOW must be within 1 day of the award

Period of Performance
The period of performance for this contract will be (b) (7)(E).
This is a 12 month period of performance.

The total obligated value of this delivery order is: \$981,005.20

All terms and conditions of both this U.S Customs and Border Protection (CBP) delivery order and the contractor's FirstSource II contract are in full effect.

Contracting Officer's Representative (COR):
Name: (b) (6), (b) (7)(C)
Tel. #: (b) (6), (b) (7)(C)
Fax #: (b) (6), (b) (7)(C)
Email: (b) (6), (b) (7)(C)@cbp.dhs.gov

The contracting point of contact for this delivery order is:
(b) (6), (b) (7)(C)
(b) (6), (b) (7)(C)@cbp.dhs.gov

Invoice Instructions
Invoices shall be submitted via IPP. See Clause ELECTRONIC INVOICING AND PAYMENT REQUIREMENTS - INVOICE PROCESSING PLATFORM (IPP) (JAN 2016) of the delivery order.

HSBP1017J00831

**ITEMS AND PRICES, DELIVERY SCHEDULE AND ACCOUNTING DATA
FOR
DELIVERY ORDER: HSBP1017J00831**

I.1 SCHEDULE OF SUPPLIES/SERVICES

| ITEM # | DESCRIPTION | QTY | UNIT | UNIT PRICE | EXT. PRICE |
|--------|-------------|---------|------|------------|------------|
| 10 | (b) (7)(E) | (b) (7) | EA | (b) (4) | |
| 20 | | (E) | EA | | |
| 30 | | | EA | | |

Total Funded Value of Award:

\$981,005.20

I.2 ACCOUNTING and APPROPRIATION DATA

| ITEM # | ACCOUNTING and APPROPRIATION DATA | AMOUNT |
|--------|--|----------------|
| 10 | 6100.315BUSCSGLCS0942715000Z00017500TT060000AE00 IU549315B TAS# 07020172017 0530000 | (b) (4) |
| 20 | 6100.315BUSCSGLCS0942715000Z00017500TT060000AE00 IU549315B TAS# 07020172017 0530000 | |
| 30 | 6100.315BUSCSGLCS0942715000Z00017500TT060000AC00 IU549315B TAS# 07020172017 0530000 | |

I.3 DELIVERY SCHEDULE

| DELIVER TO: | ITEM # | QTY | DELIVERY DATE |
|---|--------|------------|---------------|
| Customs and Border Protection (b) (7)(E) | 10 | (b) (7)(E) | (b) (7)(E) |
| | 20 | (b) (7)(E) | |
| | 30 | (b) (7)(E) | |

I.4 52.232-39 UNENFORCEABILITY OF UNAUTHORIZED OBLIGATIONS (JUN 2013)

(a) Except as stated in paragraph (b) of this clause, when any supply or service acquired under this contract is subject to any End User License Agreement (EULA), Terms of Service (TOS), or similar legal instrument or agreement, that includes any clause requiring the Government to indemnify the Contractor or any person or entity for damages, costs, fees, or any other loss or liability that would create an Anti-Deficiency Act violation (31 U.S.C. 1341), the following shall govern:

- (1) Any such clause is unenforceable against the Government.
- (2) Neither the Government nor any Government authorized end user shall be deemed to have agreed to such clause by virtue of it appearing in the EULA, TOS, or similar legal instrument or agreement. If the EULA, TOS, or similar legal instrument or agreement is invoked through an "I agree" click box or other comparable mechanism (e.g., "click-wrap" or "browse-wrap" agreements), execution does not bind the Government or any Government authorized end user to such clause.
- (3) Any such clause is deemed to be stricken from the EULA, TOS, or similar legal instrument or agreement.

(b) Paragraph (a) of this clause does not apply to indemnification by the Government that is expressly authorized by statute and specifically authorized under applicable agency regulations and procedures.

(End of clause)

I.5 52.232-40 PROVIDING ACCELERATED PAYMENTS TO SMALL BUSINESS SUBCONTRACTORS (DEC 2013)

(a) Upon receipt of accelerated payments from the Government, the Contractor shall make accelerated payments to its small business subcontractors under this contract, to the maximum extent practicable and prior to when such payment

HSBP1017J00831

is otherwise required under the applicable contract or subcontract, after receipt of a proper invoice and all other required documentation from the small business subcontractor.

- (b) The acceleration of payments under this clause does not provide any new rights under the Prompt Payment Act.
- (c) Include the substance of this clause, including this paragraph (c), in all subcontracts with small business concerns, including subcontracts with small business concerns for the acquisition of commercial items.

(End of clause)

I.6 52.203-19 PROHIBITION ON REQUIRING CERTAIN INTERNAL CONFIDENTIALITY AGREEMENTS OR STATEMENTS (JAN 2017)

I.7 52.209-10 PROHIBITION ON CONTRACTING WITH INVERTED DOMESTIC CORPORATIONS (NOV 2015)

I.8 3052.205-70 ADVERTISEMENTS, PUBLICIZING AWARDS, AND RELEASES (SEP 2012) ALTERNATE I (SEP 2012)

- (a) The Contractor shall not refer to this contract in commercial advertising or similar promotions in such a manner as to state or imply that the product or service provided is endorsed or preferred by the Federal Government or is considered by the Government to be superior to other products or services.
- (b) All advertisements, releases, announcements, or other publication regarding this contract or the agency programs and projects covered under it, or the results or conclusions made pursuant to performance, must be approved by the Contracting Officer. Under no circumstances shall the Contractor, or anyone acting on behalf of the Contractor, refer to the supplies, services, or equipment furnished pursuant to the provisions of this contract in any publicity, release, or commercial advertising without first obtaining explicit written consent to do so from the Contracting Officer.

(End of clause)

I.9 52.224-3 PRIVACY TRAINING, ALTERNATE I (DEVIATION)

- (a) Definition. As used in this clause, personally identifiable information means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. (See Office of Management and Budget (OMB) *Circular A-130, Managing Federal Information as a Strategic Resource*).
- (b) The Contractor shall ensure that initial privacy training, and annual privacy training thereafter, is completed by contractor employees who--
 - (1) Have access to a system of records;
 - (2) Create, collect, use, process, store, maintain, disseminate, disclose, dispose, or otherwise handle personally identifiable information on behalf of an agency; or
 - (3) Design, develop, maintain, or operate a system of records (see also FAR subpart 24.1 and 39.105).
- (c) The contracting agency will provide initial privacy training, and annual privacy training thereafter, to Contractor employees for the duration of this contract. Contractor employees shall satisfy this requirement by completing *Privacy at DHS: Protecting Personal Information* accessible at <http://www.dhs.gov/dhs-security-and-training-requirements-contractors>. Training shall be completed within 30 days of contract award and be completed on an annual basis thereafter not later than October 31st of each year.
- (d) The Contractor shall maintain and, upon request, provide documentation of completion of privacy training to the Contracting Officer.
- (e) The Contractor shall not allow any employee access to a system of records, or permit any employee to create, collect, use, process, store, maintain, disseminate, disclose, dispose or otherwise handle personally identifiable information, or to design, develop, maintain, or operate a system of records unless the employee has completed privacy training, as required by this clause.

HSBP1017J00831

(f) The substance of this clause, including this paragraph (f), shall be included in all subcontracts under this contract, when subcontractor employees will –

- (1) Have a system of records;
- (2) Create, collect, use, process, store, maintain, disseminate, disclose, dispose or otherwise handle personally identifiable information; or
- (3) Design, develop, maintain, or operate a system of records.

(End of clause)

I.10 PERIOD OF PERFORMANCE (MAR 2003)

The period of performance of this contract shall be from 09/21/2017 through 09/20/2018.

[End of Clause]

I.11 CONTRACTING OFFICER'S AUTHORITY (MAR 2003)

The Contracting Officer is the only person authorized to approve changes in any of the requirements of this contract. In the event the Contractor effects any changes at the direction of any person other than the Contracting Officer, the changes will be considered to have been made without authority and no adjustment will be made in the contract price to cover any increase in costs incurred as a result thereof. The Contracting Officer shall be the only individual authorized to accept nonconforming work, waive any requirement of the contract, or to modify any term or condition of the contract. The Contracting Officer is the only individual who can legally obligate Government funds. No cost chargeable to the proposed contract can be incurred before receipt of a fully executed contract or specific authorization from the Contracting Officer.

[End of Clause]

I.12 ELECTRONIC INVOICING AND PAYMENT REQUIREMENTS - INVOICE PROCESSING PLATFORM (IPP) (JAN 2016)

Beginning April 11, 2016, payment requests for all new awards must be submitted electronically through the U. S. Department of the Treasury's Invoice Processing Platform System (IPP). Payment terms for existing contracts and orders awarded prior to April 11, 2016 remain the same. The Contractor must use IPP for contracts and orders awarded April 11, 2016 or later, and must use the non-IPP invoicing process for those contracts and orders awarded prior to April 11, 2016.

"Payment request" means any request for contract financing payment or invoice payment by the Contractor. To constitute a proper invoice, the payment request must comply with the requirements identified in FAR 32.905(b), "Payment documentation and process" and the applicable Prompt Payment clause included in this contract. The IPP website address is: <https://www.ipp.gov>.

The IPP was designed and developed for Contractors to enroll, access and use IPP for submitting requests for payment. Contractor assistance with enrollment can be obtained by contacting IPPCustomerSupport@fms.treas.gov or phone (866) 973-3131.

If the Contractor is unable to comply with the requirement to use IPP for submitting invoices for payment, the Contractor must submit a waiver request in writing to the contracting officer.

(End of Clause)

I.13 GOVERNMENT CONSENT OF PUBLICATION/ENDORSEMENT (MAR 2003)

Under no circumstances shall the Contractor, or anyone acting on behalf of the Contractor, refer to the supplies, services, or equipment furnished pursuant to the provisions of this contract in any news release or commercial advertising without first obtaining explicit written consent to do so from the Contracting Officer

The Contractor agrees not to refer to awards in commercial advertising in such a manner as to state or imply that the product or service provided is endorsed or preferred by the Federal Government or is considered by the Government to be superior to other products or services.

HSBP1017J00831

[End of Clause]

I.14 SECURITY PROCEDURES (OCT 2009)**A. Controls**

1. The Contractor shall comply with the U.S. Customs and Border Protection (CBP) administrative, physical and technical security controls to ensure that the Government's security requirements are met.
2. All Government furnished information must be protected to the degree and extent required by local rules, regulations, and procedures. The Contractor shall comply with all security policies contained in CBP Handbook 1400-05C, Information Systems Security Policies and Procedures Handbook.
3. All services provided under this contract must be compliant with the Department of Homeland Security (DHS) information security policy identified in DHS Management Directive (MD) 4300.1, Information Technology Systems Security Program and DHS 4300A, Sensitive Systems Handbook.
4. All Contractor employees under this contract must wear identification access badges when working in CBP facilities. Prior to Contractor employees' departure/separation, all badges, building passes, parking permits, keys and pass cards must be given to the Contracting Officer's Technical Representative (COTR). The COTR will ensure that the cognizant Physical Security official is notified so that access to all buildings and facilities can be revoked. NOTE: For contracts within the National Capitol Region (NCR), the Office of Internal Affairs, Security Management Division (IA/SMD) should be notified if building access is revoked.
5. All Contractor employees must be registered in the Contractor Tracking System (CTS) database by the Contracting Officer (CO) or COTR. The Contractor shall provide timely start information to the CO/COTR or designated government personnel to initiate the CTS registration. Other relevant information will also be needed for registration in the CTS database such as, but not limited to, the contractor's legal name, address, brief job description, labor rate, Hash ID, schedule and contract specific information. The CO/COTR or designated government personnel shall provide the Contractor with instructions for receipt of CTS registration information. Additionally, the CO/COTR shall immediately notify IA/SMD of the contractor's departure/separation.
6. The Contractor shall provide employee departure/separation date and reason for leaving to the CO/COTR in accordance with CBP Directive 51715-006, Separation Procedures for Contractor Employees. Failure by the Contractor to provide timely notification of employee departure/separation in accordance with the contract requirements shall be documented and considered when government personnel completes a Contractor Performance Report (under Business Relations) or other performance related measures.

B. Security Background Investigation Requirements

1. In accordance with DHS Management Directive (MD) 11055, Suitability Screening Requirements for Contractors, Part VI, Policy and Procedures, Section E, Citizenship and Residency Requirements, contractor employees who require access to sensitive information must be U.S. citizens or have Lawful Permanent Resident (LPR) status. A waiver may be granted, as outlined in MD 11055, Part VI, Section M (1).
2. Contractor employees that require access to DHS IT systems or development, management, or maintenance of those systems must be U.S. citizens in accordance with MD 11055, Part VI, Section E (Lawful Permanent Resident status is not acceptable in this case). A waiver may be granted, as outlined in MD 11055, Part VI, Section M (2)
3. Provided the requirements of DHS MD 11055 are met as outlined in paragraph 1, above, contractor employees requiring access to CBP facilities, sensitive information or information technology resources are required to have a favorably adjudicated background investigation (BI) or a single scope background investigation (SSBI) prior to commencing work on this contract. Exceptions shall be approved on a case-by-case basis with the employee's access to facilities, systems, and information limited until the Contractor employee receives a favorably adjudicated BI or SSBI. A favorable adjudicated BI or SSBI shall include various aspects of a Contractor employee's life, including employment, education, residences, police and court inquires, credit history, national agency checks, and a CBP Background Investigation Personal Interview (BIPI).
4. The Contractor shall submit within ten (10) working days after award of this contract a list containing the full name, social security number, place of birth (city and state), and date of birth of employee candidates who possess

HSBP1017J00831

favorably adjudicated BI or SSBI that meets federal investigation standards.. For employee candidates needing a BI for this contract, the Contractor shall require the applicable employees to submit information and documentation requested by CBP to initiate the BI process.

5. Background Investigation information and documentation is usually submitted by completion of standard federal and agency forms such as Questionnaire for Public Trust and Selected Positions or Questionnaire for National Security Positions; Fingerprint Chart; Fair Credit Reporting Act (FCRA) form; Criminal History Request form; and Financial Disclosure form. These forms must be submitted to the designated CBP official identified in this contract. The designated CBP security official will review the information for completeness.
6. The estimated completion of a BI or SSBI is approximately sixty (60) to ninety (90) days from the date of receipt of the properly completed forms by CBP security office. During the term of this contract, the Contractor is required to provide the names of contractor employees who successfully complete the CBP BI or SSBI process. Failure of any contractor employee to obtain and maintain a favorably adjudicated BI or SSBI shall be cause for dismissal. For key personnel, the Contractor shall propose a qualified replacement employee candidate to the CO and COTR within 30 days after being notified of an unsuccessful candidate or vacancy. For all non-key personnel contractor employees, the Contractor shall propose a qualified replacement employee candidate to the COTR within 30 days after being notified of an unsuccessful candidate or vacancy. The CO/COTR shall approve or disapprove replacement employees. Continuous failure to provide contractor employees who meet CBP BI or SSBI requirements may be cause for termination of the contract.

C. Security Responsibilities

1. The Contractor shall ensure that its employees follow the general procedures governing physical, environmental, and information security described in the various DHS CBP regulations identified in this clause. The contractor shall ensure that its employees apply proper business practices in accordance with the specifications, directives, and manuals required for conducting work under this contract. Applicable contractor personnel will be responsible for physical security of work areas and CBP furnished equipment issued under this contract.
2. The CO/COTR may require the Contractor to prohibit its employees from working on this contract if continued employment becomes detrimental to the public's interest for any reason including, but not limited to carelessness, insubordination, incompetence, or security concerns.
3. Work under this contract may require access to sensitive information as defined under Homeland Security Acquisition Regulation (HSAR) Clause 3052.204-71, Contractor Employee Access, included in the solicitation/contract. The Contractor shall not disclose, orally or in writing, any sensitive information to any person unless authorized in writing by the CO.
4. The Contractor shall ensure that its employees who are authorized access to sensitive information, receive training pertaining to protection and disclosure of sensitive information. The training shall be conducted during and after contract performance.
5. Upon completion of this contract, the Contractor shall return all sensitive information used in the performance of the contract to the CO/COTR. The Contractor shall certify, in writing, that all sensitive and non-public information has been purged from any Contractor-owned system.

D. Notification of Contractor Employee Changes

1. The Contractor shall notify the CO/COTR via phone, facsimile, or electronic transmission, immediately after a personnel change become known or no later than five (5) business days prior to departure of the employee. Telephone notifications must be immediately followed up in writing. Contractor's notification shall include, but is not limited to name changes, resignations, terminations, and reassignments to another contract.
2. The Contractor shall notify the CO/COTR and program office (if applicable) in writing of any proposed change in access requirements for its employees at least fifteen (15) days, or thirty (30) days if a security clearance is to be obtained, in advance of the proposed change. The CO/COTR will notify the Office of Information and Technology (OIT) Information Systems Security Branch (ISSB) of the proposed change. If a security clearance is required, the CO/COTR will notify IA/SMD.

E. Non-Disclosure Agreements

HSBP1017J00831

When determined to be appropriate, Contractor employees are required to execute a non-disclosure agreement (DHS Form 11000-6) as a condition to access sensitive but unclassified information.

[End of Clause]

I.15 SPECIAL SECURITY REQUIREMENT - CONTRACTOR PRE-SCREENING (SEP 2011)

1. Contractors requiring recurring access to Government facilities or access to sensitive but unclassified information and/or logical access to Information Technology (IT) resources shall verify minimal fitness requirements for all persons/candidates designated for employment under any Department of Security (DHS) contract by pre-screening the person /candidate prior to submitting the name for consideration to work on the contract. Pre-screening the candidate ensures that minimum fitness requirements are considered and mitigates the burden of DHS having to conduct background investigations on objectionable candidates. The Contractor shall submit only those candidates that have not had a felony conviction within the past 36 months or illegal drug use within the past 12 months from the date of submission of their name as a candidate to perform work under this contract. Contractors are required to flow this requirement down to subcontractors. Pre-screening involves contractors and subcontractors reviewing:
 - a. Felony convictions within the past 36 months. An acceptable means of obtaining information on felony convictions is from public records, free of charge, or from the National Crime Information Center (NCIC).
 - b. Illegal drug use within the past 12 months. An acceptable means of obtaining information related to drug use is through employee self certification, by public records check; or if the contractor or subcontractor already has drug testing in place. There is no requirement for contractors and/or subcontractors to initiate a drug testing program if they do not have one already in place.
 - c. Misconduct such as criminal activity on the job relating to fraud or theft within the past 12 months. An acceptable means of obtaining information related to misconduct is through employee self certification, by public records check, or other reference checks conducted in the normal course of business.
2. Pre-screening shall be conducted within 15 business days after contract award. This requirement shall be placed in all subcontracts if the subcontractor requires routine physical access, access to sensitive but unclassified information, and/or logical access to IT resources. Failure to comply with the pre-screening requirement will result in the Contracting Officer taking the appropriate remedy.

Definition: *Logical Access* means providing an authorized user the ability to access one or more computer system resources such as a workstation, network, application, or database through automated tools. A logical access control system (LACS) requires validation of an individual identity through some mechanism such as a personal identification number (PIN), card, username and password, biometric, or other token. The system has the capability to assign different access privileges to different persons depending on their roles and responsibilities in an organization.

[End of Clause]



**Homeland
Security**

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

Privacy Threshold Analysis
Version number: 01-2014
Page 1 of 12

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



Homeland Security

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

Privacy Threshold Analysis
Version number: 01-2014
Page 2 of 12

PRIVACY THRESHOLD ANALYSIS (PTA) SUMMARY INFORMATION

| | | | |
|--|---|---|-----------------------------|
| Project or Program Name: | ESTA Social Media Tool Pilot Evaluation | | |
| Component: | CBP | Office or Program: | OFC (b) (7) (C) |
| 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: | June 15, 2016 | Pilot launch date: | July 11, 2016 |
| Date of last PTA update | Click here to enter a date. | Pilot end date: | December 31, 2016 |
| 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) (6), (b) (7)(C) | | |
| Phone: | (b) (6), (b) (7)(C) | Email: | (b) (6), (b) (7)(C)@associates.dhs.gov |



Homeland Security

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

Privacy Threshold Analysis
Version number: 01-2014
Page 3 of 12

SPECIFIC PTA QUESTIONS

1. Reason for submitting the PTA: New PTA

The Department of Homeland Security (DHS), U.S. Customs and Border Protection, is responsible for border security while facilitating legitimate travel and trade. CBP has broad authority to vet Electronic System for Travel Authorization (ESTA) applications against various data, including open source and publicly available information derived from social media, to accomplish its border security mission. *See e.g.*, Implementing Recommendations of the 9/11 Commission Act of 2007, Public Law 110-53; Visa Waiver Program Improvement and Terrorist Travel Prevention Act of 2015; Title IV of the Homeland Security Act of 2002, as amended by section 802 of the Trade Facilitation and Trade Enforcement Act of 2015; the Immigration and Naturalization Act, as amended, including 8 U.S.C. 1187(a)(11) and (h)(3), and implementing regulations contained in part 217, title 8, Code of Federal Regulations; the Travel Promotion Act of 2009, Public Law 111-145, 22 U.S.C. 2131; 19 U.S.C. 482, 1467, 1496, 1582, and 1589a.

CBP is entering into a testing and evaluation pilot with the DHS Science and Technology (S&T) Directorate to test and evaluate tools (b) (7)(E) social media for screening and vetting of Electronic System for Travel Authorization (ESTA) applicants. CBP currently accesses publicly available social media, consistent with a previously approved Social Media Operational Use Template (SMOUT), which permits CBP to use masked monitoring techniques (described below) to manually screen and vet ESTA applicants. This test and evaluation process does not expand on the types of open source and publicly available information derived from social media information already used by CBP under their inspection authorities.

This initial phase of the pilot project will only cover approximately (b) (7)(E)

(b) (7)(E)

CBP will conduct screening and vetting of ESTA applicants but will not conduct screening and vetting of

(b) (7)(E)

Tools used during the pilot (S&T is in the process of conducting its own PTAs for the Social Media Vetting tools):

1. (b) (4), (b) (7)(E)



Homeland Security

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

Privacy Threshold Analysis
Version number: 01-2014

Page 4 of 12

2. (b) (4), (b) (7)(E)

For this pilot, information regarding ESTA applicants will be loaded into the (b) (4), (b) (7)(E) for use by CBP Officers and S&T contracting staff (with CBP officer oversight). All searches and information collected will be done under CBP law enforcement authorities, consistent with the approved SMOUT. S&T contractors will not adjudicate any results. Employees from (b) (4), (b) (7)(E)

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

S&T will leverage its contracts to provide analysts and language analysts to support CBP Officers, if needed. S&T will only use information regarding the process to improve technical performance of systems, tools and algorithms and will not use any information collected for any operational purposes.

In all cases, CBP will access publicly available information in accordance with its authorities and the privacy policies of the underlying platform. This means that all searches will be conducted using open source material and that CBP Officers must respect individuals' privacy settings and access only information that is publicly available, and cannot "friend, fan, or like" any individuals. (b) (4), (b) (7)(E)

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

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

| | |
|---|--|
| <p>2. Does this system employ any of the following technologies:</p> <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> | <p><input type="checkbox"/> Closed Circuit Television (CCTV)</p> <p><input checked="" type="checkbox"/> Social Media</p> <p><input type="checkbox"/> Web portal¹ (e.g., SharePoint)</p> <p><input type="checkbox"/> Contact Lists</p> <p><input type="checkbox"/> None of these</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.



Homeland Security

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

Privacy Threshold Analysis
Version number: 01-2014
Page 5 of 12

| | |
|---|--|
| <p>3. From whom does the Project or Program collect, maintain, use, or disseminate information?</p> <p><i>Please check all that apply.</i></p> | <p><input type="checkbox"/> This program does not collect any personally identifiable information²</p> <p><input checked="" type="checkbox"/> Members of the public</p> <p><input type="checkbox"/> DHS employees/contractors (list components):</p> <p><input type="checkbox"/> Contractors working on behalf of DHS</p> <p><input type="checkbox"/> Employees of other federal agencies</p> |
|---|--|

| |
|--|
| <p>4. What specific information about individuals is collected, generated or retained?</p> |
| <p>(b) (7)(E)</p> <p>As part of this pilot, CBP will also collect publicly available information from social media platforms to assess the admissibility of ESTA applicants. Any derogatory information collected from social media and deemed operationally necessary will be stored in the Automated Targeting System (ATS).</p> <p>The full list of ESTA application fields is below:</p> <ul style="list-style-type: none"> • Full name (first, middle, and last); • Other names or aliases, if available; • Date of birth; • City and country of birth; • Gender; • Email address; • Telephone number (home, mobile, work, other); • Home address (address, apartment number, city, state/region); • Internet protocol (IP) address; • ESTA application number; • Country of residence; |

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.



Homeland Security

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

Privacy Threshold Analysis
Version number: 01-2014
Page 6 of 12

| | |
|--|--|
| <ul style="list-style-type: none"> • Passport number; • Passport issuing country; • Passport issuance date; • Passport expiration date; • Country of citizenship; • Other citizenship (country, passport number); • National identification number, if available; • Address while visiting the United States (number, street, city, state); • Emergency point of contact information (name, telephone number, email address); and, • U.S. Point of Contact (name, address, telephone number). • Parents' names; • Current job title; • Current or previous employer name; • Current or previous employer street address; and • Current or previous employer telephone number. | |
| <p>4(a) Does the project, program, or system retrieve information by personal identifier?</p> | <p><input type="checkbox"/> No. Please continue to next question.</p> <p><input checked="" type="checkbox"/> Yes. If yes, please list all personal identifiers used: (b) (7)(E)</p> <p>██████████</p> <p>██████████</p> |
| <p>4(b) Does the project, program, or system use Social Security Numbers (SSN)?</p> | <p><input checked="" type="checkbox"/> No.</p> <p><input type="checkbox"/> Yes.</p> |
| <p>4(c) If yes, please provide the specific legal basis and purpose for the collection of SSNs:</p> | <p>N/A</p> |
| <p>4(d) If yes, please describe the uses of the SSNs within the project, program, or system:</p> | <p>N/A</p> |
| <p>4(e) If this project, program, or system is an information technology/system, does it relate solely to infrastructure?</p> <p><i>For example, is the system a Local Area Network (LAN) or Wide Area Network (WAN)?</i></p> | <p><input checked="" type="checkbox"/> No. Please continue to next question.</p> <p><input type="checkbox"/> Yes. If a log kept of communication traffic, please answer the following question.</p> |



Homeland Security

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

Privacy Threshold Analysis
Version number: 01-2014
Page 7 of 12

| |
|---|
| 4(f) If header or payload data³ is stored in the communication traffic log, please detail the data elements stored. |
| N/A |

| | |
|--|--|
| 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: PII for ESTA applications is provided by CBP (b) (7)(E) S&T to facilitate the pilot. (b) (7)(E) _____ |
| 6. Does this project, program, or system connect, receive, or share PII with any external (non-DHS) partners or systems⁴? | <input type="checkbox"/> No. <input checked="" type="checkbox"/> Yes. If yes, please list: (b) (4), (b) (7)(E) |
| 6(a) Is this external sharing pursuant to new or existing information sharing access agreement (MOU, MOA, LOI, etc.)? | (b) (4), (b) (7)(E) Please describe applicable information sharing governance in place: |
| 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 checked="" type="checkbox"/> No. <input type="checkbox"/> Yes. If yes, please list: |
| 8. -Per NIST SP 800-53 Rev. 4, Appendix J, does the project, program, or system maintain an accounting of disclosures of PII to | <input checked="" type="checkbox"/> No. What steps will be taken to develop and maintain the accounting: (b) (4), (b) (7)(E) |

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.



Homeland Security

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

Privacy Threshold Analysis
Version number: 01-2014
 Page 8 of 12

| | |
|---|--|
| individuals/agencies who have requested access to their PII? | (b) (4), (b) (7)(E) |
| | <input type="checkbox"/> Yes. In what format is the accounting maintained: |
| 9. Is there a FIPS 199 determination?⁵ | <input type="checkbox"/> Unknown. <input type="checkbox"/> No. <input checked="" type="checkbox"/> Yes. Please indicate the determinations for each of the following: Confidentiality: <input type="checkbox"/> Low <input checked="" type="checkbox"/> Moderate <input type="checkbox"/> High <input type="checkbox"/> Undefined Integrity: <input checked="" type="checkbox"/> Low <input type="checkbox"/> Moderate <input type="checkbox"/> High <input type="checkbox"/> Undefined Availability: <input checked="" type="checkbox"/> Low <input type="checkbox"/> Moderate <input type="checkbox"/> High <input type="checkbox"/> Undefined |

PRIVACY THRESHOLD REVIEW

(TO BE COMPLETED BY COMPONENT PRIVACY OFFICE)

| | |
|--|----------------------------|
| Component Privacy Office Reviewer: | (b) (6), (b) (7)(C) |
| Date submitted to Component Privacy Office: | June 21, 2016 |
| Date submitted to DHS Privacy Office: | July 7, 2016 |
| 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] | |

⁵ FIPPS 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
202-343-1717, pia@dhs.gov
www.dhs.gov/privacy

Privacy Threshold Analysis
Version number: 01-2014
Page 9 of 12

(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: | 1127636 |
| Date approved by DHS Privacy Office: | July 8, 2016 |
| PTA Expiration Date | July 8, 2019 |

DESIGNATION



Homeland Security

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

Privacy Threshold Analysis
Version number: 01-2014
Page 10 of 12

| | |
|--|---|
| 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 DHS/CBP/PIA-006(b) Automated Targeting System (ATS) Update, June 1, 2012 |
| SORN: | System covered by existing SORN DHS/CBP-006 - Automated Targeting System May 22, 2012, 77 FR 30297 |
| DHS Privacy Office Comments: | |
| <i>Please describe rationale for privacy compliance determination above.</i> | |
| <p>The DHS Privacy Office finds that the ESTA Social Media Tool Pilot Evaluation is Privacy Sensitive and requires both PIA and SORN coverage. The pilot, representing a joint effort between U.S. Customs and Border Protection (CBP) and the DHS Science and Technology (S&T) Directorate, involves the testing and evaluation of tools (b) (7)(E) the use of social media for the screening and vetting of Electronic System for Travel Authorization (ESTA) applicants. (b) (7)(E)</p> <p>(b) (7)(E)</p> <p>(b) (7)(E)</p> <p>(b) (7)(E)</p> <p>(b) (7)(E)</p> <p>(b) (7)(E)</p> <p>(b) (7)(E)</p> <p>(b) (7)(E)</p> <p>(b) (7)(E)</p> <p>(b) (7)(E)</p> <p>(b) (7)(E)</p> | |
| <p>The Privacy Office agrees with CBP's assertion that PIA coverage for the ESTA Social Media Tools Pilot is provided under DHS/CBP/PIA-006(b) Automated Targeting System (ATS) Update, June 1, 2012, which outlines CBP's use of decision support tools in order to compare traveler information against law enforcement, intelligence, and other enforcement data. Additionally, DHS/CBP/PIA-006(b) outlines the querying of publicly available information on the internet in support of the vetting process. PRIV also</p> | |



Homeland Security

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

Privacy Threshold Analysis
Version number: 01-2014
Page 11 of 12

agrees that SORN coverage falls under DHS/CBP-006 - Automated Targeting System, which notes that CBP collects information on individuals whom may be subject to closer questioning or examination upon arrival to or departure from the United States or who may require further examination, as well as those who may pose a risk to border security or public safety, may be a terrorist or suspected terrorist, or may otherwise be engaged in activity in violation of U.S. law. (b) (5)

[REDACTED]



**Homeland
Security**

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

Privacy Threshold Analysis
Version number: 01-2014
Page 1 of 12

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.



Homeland Security

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

Privacy Threshold Analysis
Version number: 01-2014
Page 2 of 12

PRIVACY THRESHOLD ANALYSIS (PTA)

SUMMARY INFORMATION

| | | | |
|--|---|---|-----------------------------|
| Project or Program Name: | ESTA Social Media Tool Pilot Evaluation, Update 3 | | |
| 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: | June 15, 2016 | Pilot launch date: | July 11, 2016 |
| Date of last PTA update | November 21, 2016 | 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) (CBP) | | |
| Office: | OFO | Title: | Director |
| Phone: | (b) (6), (b) (7)(C) | Email: | (b) (6), (b) (7)(C)@cbp.dhs.gov |

INFORMATION SYSTEM SECURITY OFFICER (ISSO) (IF APPLICABLE)

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



SPECIFIC PTA QUESTIONS

1. Reason for submitting the PTA: Updated PTA

CBP is updating the previously submitted ESTA Social Media Pilot PTA to expand the previously approved population for vetting, and to expand the suite of social media tools for testing.

Expanded Population

At secondary inspection, CBP regularly identifies new individuals who (b) (7)(E)

(b) (7)(E)

(b) (7)(E)

Expanded Social Media Vetting Tools, in addition to (b) (7)(E)

S&T continues to test open source and social media tools for the Department. *All of the social media tools being tested have the same function: to collect open source and social media data based on DHS mission requirements.* DHS S&T is evaluating the features, functionality and performance of each suite of tools. The underlying PII used is substantially the same from one suite of tools to the next. S&T and CBP may jointly test other tools identified by S&T's assessment of over 275 social media tools. The assessment will continually be updated to identify new capabilities for DHS. The rules and understanding established by this PTA will apply to the piloting of the other tools. Potential tools include:

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



**Homeland
Security**

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

Privacy Threshold Analysis
Version number: 01-2014
Page 4 of 12

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



Homeland Security

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

Privacy Threshold Analysis
Version number: 01-2014
Page 5 of 12

In addition, the next phase of the ESTA pilot will continue to test online (b) (7)(E) such as (b) (4), (b) (7)(E) for the federal government (b) (7)(E) was used in the original ESTA pilot. (b) (7)(E)
(b) (7)(E)

In all cases, CBP will access publicly available information in accordance with its authorities and the privacy policies of the underlying platform. (b) (7)(E)

Data within the social media tools is only made available to users in accordance with the privacy policy of the underlying data source.

| | |
|---|--|
| <p>2. Does this system employ any of the following technologies: <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> | <p><input type="checkbox"/> Closed Circuit Television (CCTV)</p> <p><input checked="" type="checkbox"/> Social Media</p> <p><input type="checkbox"/> Web portal¹ (e.g., SharePoint)</p> <p><input type="checkbox"/> Contact Lists</p> <p><input type="checkbox"/> None of these</p> |
|---|--|

| | |
|---|--|
| <p>3. From whom does the Project or Program collect, maintain, use, or disseminate information? <i>Please check all that apply.</i></p> | <p><input type="checkbox"/> This program does not collect any personally identifiable information²</p> <p><input checked="" type="checkbox"/> Members of the public</p> <p><input type="checkbox"/> DHS employees/contractors (list components):</p> <p><input type="checkbox"/> Contractors working on behalf of DHS</p> <p><input type="checkbox"/> Employees of other federal agencies</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.



Homeland Security

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

Privacy Threshold Analysis
Version number: 01-2014
Page 6 of 12

4. What specific information about individuals is collected, generated or retained?

(b) (7)(E)

[REDACTED]

[REDACTED]. As part of this pilot, CBP will also collect publicly available information from social media platforms to assess the admissibility of ESTA applicants. Any derogatory information collected from social media and deemed operationally necessary will be stored in the Automated Targeting System (ATS), (b) (7)(E) [REDACTED]

[REDACTED] Consistent with the ESTA PIA, while the information may be used to make an admissibility determination, DHS/CBP does not intend to maintain such third-party information as part of the ESTA application, and any such collection will be within the scope of an authorized law enforcement activity, as permitted by subsection (e)(7). For example, (b) (7)(E) [REDACTED]

[REDACTED]

[REDACTED]

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

Expanded Population:
During recent secondary inspections CBP has identified individuals at ports-of-entry (b) (7)(E)

(b) (7) (E)



Homeland Security

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

Privacy Threshold Analysis
Version number: 01-2014
 Page 7 of 12

| | |
|---|---|
| <p>4(a) Does the project, program, or system retrieve information by personal identifier?</p> | <p><input type="checkbox"/> No. Please continue to next question. <input checked="" type="checkbox"/> Yes. If yes, please list all personal identifiers used: All ESTA application fields (b) (7)(E) (b) (7)(E)</p> |
| <p>4(b) Does the project, program, or system use Social Security Numbers (SSN)?</p> | <p><input checked="" type="checkbox"/> No. <input type="checkbox"/> Yes.</p> |
| <p>4(c) If yes, please provide the specific legal basis and purpose for the collection of SSNs:</p> | <p>Click here to enter text.</p> |
| <p>4(d) If yes, please describe the uses of the SSNs within the project, program, or system:</p> | <p>Click here to enter text.</p> |
| <p>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></p> | <p><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.</p> |
| <p>4(f) If header or payload data³ is stored in the communication traffic log, please detail the data elements stored.</p> | |
| <p>Click here to enter text.</p> | |

| | |
|---|--|
| <p>5. Does this project, program, or system connect, receive, or share PII with any other DHS programs or systems⁴?</p> | <p><input type="checkbox"/> No. <input checked="" type="checkbox"/> Yes. If yes, please list: For the initial pilot that ended September 9, 2016, PII for ESTA applications was provided by CBP (b) (7)(E) to S&T to facilitate the pilot. There were no connections between the pilot system and other DHS systems.</p> |
|---|--|

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.



Homeland Security

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

Privacy Threshold Analysis
Version number: 01-2014
Page 8 of 12

| | |
|---|--|
| | <p>For the operational pilot beginning November 2016, CBP will (b) (7)(E)</p> <p>(b) (7)(E)</p> |
| <p>6. Does this project, program, or system connect, receive, or share PII with any external (non-DHS) partners or systems?</p> | <p><input type="checkbox"/> No.</p> <p><input checked="" type="checkbox"/> Yes. If yes, please list: Information from ESTA applications is (b) (7)(E) (b) (7)(E) At the conclusion of the operational pilot, the social media tools will destroy all data within 2 days after the pilot has been completed and certify that all CBP data has been deleted.</p> |
| <p>6(a) Is this external sharing pursuant to new or existing information sharing access agreement (MOU, MOA, LOI, etc.)?</p> | <p>Existing.</p> <p>Please describe applicable information sharing governance in place.</p> |
| <p>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?</p> | <p><input checked="" type="checkbox"/> No.</p> <p><input type="checkbox"/> Yes. If yes, please list:</p> |
| <p>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?</p> | <p><input checked="" type="checkbox"/> No. What steps will be taken to develop and maintain the accounting: CBP and S&T are disclosing information to vendors (b) (4), (b) (7)(E)</p> <p>The other vendors will be treated accordingly when a contract or CRADA is in place.</p> |



Homeland Security

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

Privacy Threshold Analysis
Version number: 01-2014
Page 9 of 12

| | |
|--|--|
| | (b) (4), (b) (7)(E) |
| | <input type="checkbox"/> Yes. In what format is the accounting maintained: |
| 8. Is there a FIPS 199 determination?⁴ | <input type="checkbox"/> Unknown. <input type="checkbox"/> No. <input checked="" type="checkbox"/> Yes. Please indicate the determinations for each of the following: (The reference is for S&T's Data Analytics laboratory, which brings in many tools for evaluation for various projects.) Confidentiality: <input type="checkbox"/> Low <input checked="" type="checkbox"/> Moderate <input type="checkbox"/> High <input type="checkbox"/> Undefined Integrity: <input checked="" type="checkbox"/> Low <input type="checkbox"/> Moderate <input type="checkbox"/> High <input type="checkbox"/> Undefined Availability: <input checked="" type="checkbox"/> Low <input type="checkbox"/> Moderate <input type="checkbox"/> High <input type="checkbox"/> Undefined |

PRIVACY THRESHOLD REVIEW

(TO BE COMPLETED BY COMPONENT PRIVACY OFFICE)

| | |
|---|----------------------------|
| Component Privacy Office Reviewer: | (b) (6), (b) (7)(C) |
|---|----------------------------|

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



Homeland Security

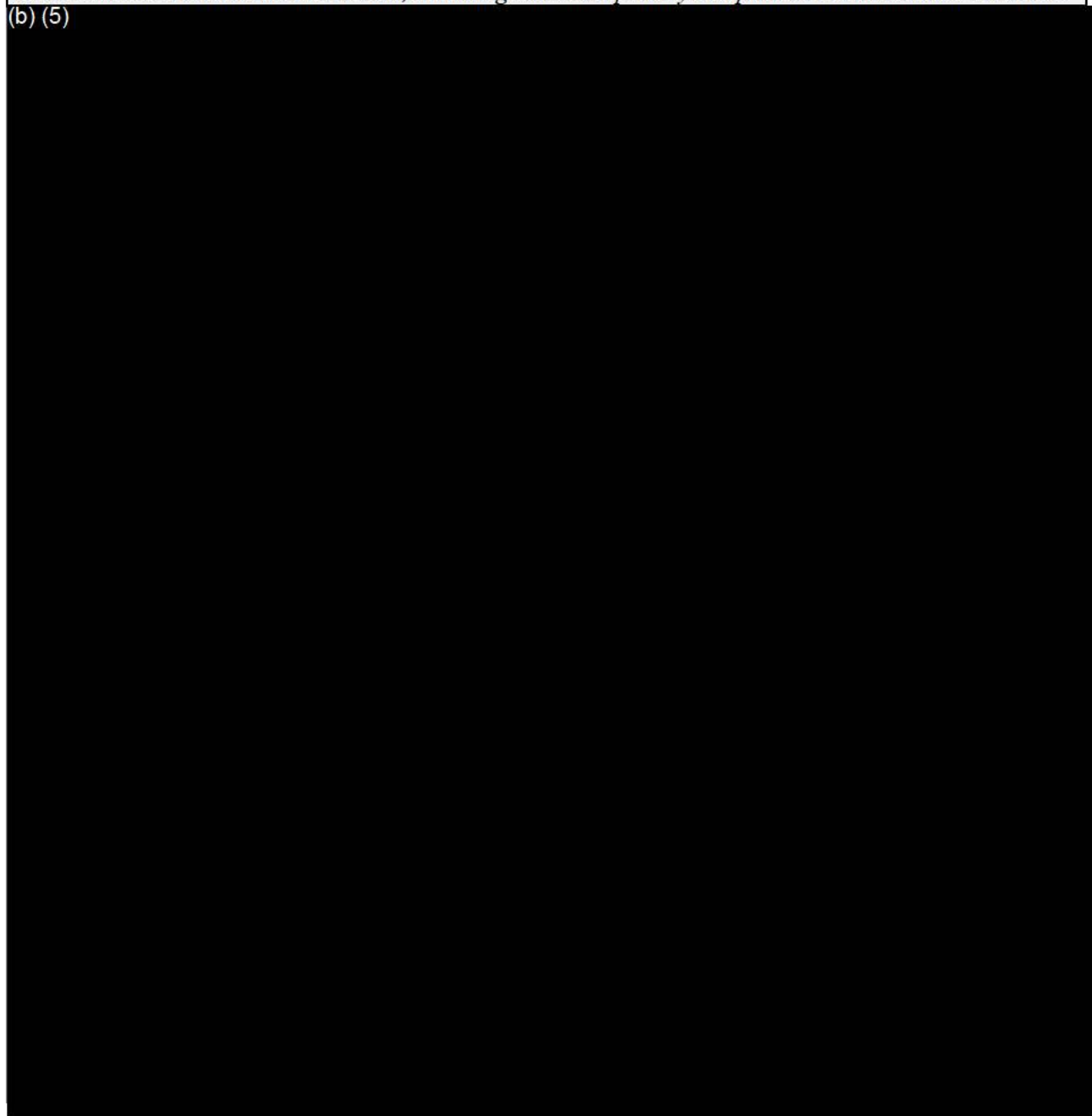
Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
202-343-1717, pia@dhs.gov
www.dhs.gov/privacy

Privacy Threshold Analysis
Version number: 01-2014
Page 10 of 12

| | |
|--|----------------------|
| Date submitted to Component Privacy Office: | March 1, 2017 |
| Date submitted to DHS Privacy Office: | April 14, 2017 |

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

(b) (5)





Homeland Security

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

Privacy Threshold Analysis
Version number: 01-2014
Page 11 of 12

(TO BE COMPLETED BY THE DHS PRIVACY OFFICE)

| | |
|---|---------------------|
| DHS Privacy Office Reviewer: | (b) (6), (b) (7)(C) |
| PCTS Workflow Number: | 1142082 |
| Date approved by DHS Privacy Office: | May 9, 2017 |
| PTA Expiration Date | December 31, 2017 |

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: | PIA in progress If covered by existing PIA, please list: (b) (6), (b) (7)(C) CBP PIA coverage is provided by: DHS/CBP/PIA-006(b) Automated Targeting System (ATS) DHS/CBP/PIA-007(g) Electronic System for Travel Authorization (ESTA) |
| SORN: | SORN update is required. If covered by existing SORN, please list: DHS/S&T-001 Research, Development, Test, and Evaluation Records, January 15, 2013, 78 FR 3019 should be updated to include minimum Social Media handles. CBP SORN coverages is provided by: |



Homeland Security

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

Privacy Threshold Analysis

Version number: 01-2014

Page 12 of 12

| | |
|--|---|
| | <p>DHS/CBP-006 Automated Targeting System, May 22, 2012, 77 FR 30297 DHS/CBP-009 Electronic System for Travel Authorization, September 2, 2016, 81 FR 60713</p> |
| <p>DHS Privacy Office Comments: <i>Please describe rationale for privacy compliance determination above.</i></p> | |
| <p>CBP is submitting this PTA to discuss the next update for the ESTA Social Media Pilot. The pilot, representing a joint effort between CBP and S&T, involves the testing and evaluation of tools (b) (7)(E) the use of social media for the screening and vetting of ESTA applicants. The next phase of the pilot expands the previously approved population for vetting and the suite of social media tools for testing.</p> <p>The DHS Privacy Office finds that this phase of the pilot is privacy-sensitive, requiring both PIA and SORN coverage.</p> <p>(b) (7)(E)</p> <p>S&T SORN coverage is required because the S&T evaluation of social media vetting tools will retrieve information by a unique identifier. The DHS Privacy Office finds that the DHS/S&T-001 Research, Development, Test, and Evaluation Records SORN needs to be updated to include at minimum social media handles. The DHS Privacy Office recognizes S&T Research, Development, Test, and Evaluation records vary according to specific project, and S&T should not be using social media for operational purposes, yet social media handles are collected and therefore must update the SORN.</p> <p>CBP coverage for participation of this pilot is covered by DHS/CBP/PIA-007 ESTA and the DHS/CBP-009 ESTA SORN, which was recently updated to include social media identifiers. The Privacy Office agrees that coverage for this pilot is also provided under DHS/CBP/PIA-006 ATS, which outlines CBP's use of decision support tools in order to compare traveler information against law enforcement, intelligence, and other enforcement data. Additionally, this PIA outlines the querying of publicly available information in support of the vetting process. The DHS Privacy Office also agrees that SORN coverage is provided by the DHS/CBP-006 ATS SORN, which notes that CBP collects information on individuals whom may be subject to closer questioning or examination upon arrival to or departure from the United States or who may require further examination, as well as those who may pose a risk to border security or public safety, may be a terrorist or suspected terrorist, or may otherwise be engaged in activity in violation of U.S. law.</p> <p>In all cases, CBP will access publicly available information in accordance with its authorities and the privacy policies of the underlying platform. This means that all searches will be conducted using open source material and that CBP Officers must respect individuals' privacy settings and access only information that is publicly available, (b) (7)(E). Data within the social media tools is only made available to users in accordance with the privacy policy of the underlying data source.</p> <p>This PTA expires with the pilot end date on December 31, 2017. The S&T privacy compliance documentation requirements do not impede pilot operations.</p> | |



**Homeland
Security**

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

Privacy Threshold Analysis
Version number: 01-2014
Page 1 of 10

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.



Homeland Security

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

Privacy Threshold Analysis
Version number: 01-2014
Page 2 of 10

PRIVACY THRESHOLD ANALYSIS (PTA)

SUMMARY INFORMATION

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

PROJECT OR PROGRAM MANAGER

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

INFORMATION SYSTEM SECURITY OFFICER (ISSO) (IF APPLICABLE)

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



Homeland Security

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

Privacy Threshold Analysis
Version number: 01-2014
Page 3 of 10

SPECIFIC PTA QUESTIONS

1. Reason for submitting the PTA: New PTA

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

(b) (7)(E)

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

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

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



Homeland Security

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

Privacy Threshold Analysis
Version number: 01-2014
Page 5 of 10

| | |
|--|---|
| <p>The full list of ESTA application fields is below:</p> <ul style="list-style-type: none"> • Full name (first, middle, and last); • Other names or aliases, if available; • Date of birth; • City and country of birth; • Gender; • Email address; • Telephone number (home, mobile, work, other); • Home address (address, apartment number, city, state/region); • Internet protocol (IP) address; • ESTA application number; • Country of residence; • Social media handles | |
| <p>4(a) Does the project, program, or system retrieve information by personal identifier?</p> | <p><input type="checkbox"/> No. Please continue to next question. <input checked="" type="checkbox"/> Yes. If yes, please list all personal identifiers used: (b) (7)(E)</p> |
| <p>4(b) Does the project, program, or system use Social Security Numbers (SSN)?</p> | <p><input checked="" type="checkbox"/> No. <input type="checkbox"/> Yes.</p> |
| <p>4(c) If yes, please provide the specific legal basis and purpose for the collection of SSNs:</p> | <p>Click here to enter text.</p> |
| <p>4(d) If yes, please describe the uses of the SSNs within the project, program, or system:</p> | <p>Click here to enter text.</p> |
| <p>4(e) If this project, program, or system is an information technology/system, does it relate solely to infrastructure?</p> <p><i>For example, is the system a Local Area Network (LAN) or Wide Area Network (WAN)?</i></p> | <p><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.</p> |
| <p>4(f) If header or payload data³ is stored in the communication traffic log, please detail the data elements stored.</p> | |
| <p>Click here to enter text.</p> | |

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.



Homeland Security

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

Privacy Threshold Analysis
Version number: 01-2014
Page 6 of 10

| | |
|---|---|
| <p>5. Does this project, program, or system connect, receive, or share PII with any other DHS programs or systems⁴?</p> | <p><input type="checkbox"/> No. <input checked="" type="checkbox"/> Yes. If yes, please list: Any PII or potentially derogatory information identified and retained will be stored within ATSTF.</p> |
| <p>6. Does this project, program, or system connect, receive, or share PII with any external (non-DHS) partners or systems?</p> | <p><input type="checkbox"/> No. <input checked="" type="checkbox"/> Yes. If yes, please list: Information regarding ESTA applications will be loaded into (b) (7)(E) (b) (7)(E)</p> |
| <p>6(a) Is this external sharing pursuant to new or existing information sharing access agreement (MOU, MOA, LOI, etc.)?</p> | <p>Existing Please describe applicable information sharing governance in place: (b) (7)(E) (b) (7)(E)</p> |
| <p>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?</p> | <p><input type="checkbox"/> No. <input checked="" type="checkbox"/> Yes. If yes, please list: All CBP Officers, Agents, Analysts, and Contractors using Social Media for operational purposes must complete the CBP Social Media Training and Rules of Behavior. (b) (7)(E)</p> |



Homeland Security

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

Privacy Threshold Analysis
Version number: 01-2014
Page 7 of 10

| | |
|---|--|
| <p>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?</p> | <p><input checked="" type="checkbox"/> No. What steps will be taken to develop and maintain the accounting:</p> <div style="background-color: black; color: white; text-align: center; padding: 20px; font-size: 2em; font-weight: bold;">(b) (7)(E)</div> <p><input type="checkbox"/> Yes. In what format is the accounting maintained:</p> |
| <p>9. Is there a FIPS 199 determination?⁴</p> | <p><input type="checkbox"/> Unknown. <input type="checkbox"/> No. <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 type="checkbox"/> Low <input checked="" type="checkbox"/> Moderate <input type="checkbox"/> High <input type="checkbox"/> Undefined</p> <p>Availability: <input type="checkbox"/> Low <input checked="" 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: | December 6, 2017 |

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



Homeland Security

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

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

| | |
|--|-------------------|
| Date submitted to DHS Privacy Office: | December 20, 2017 |
| Component Privacy Office Recommendation: | |
| <i>Please include recommendation below, including what new privacy compliance documentation is needed.</i> | |
| (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: | 1155460 |
| Date approved by DHS Privacy Office: | January 5, 2018 |
| PTA Expiration Date | January 5, 2021 |

DESIGNATION

| | |
|----------------------------------|---|
| Privacy Sensitive System: | Yes If “no” PTA adjudication is complete. |
| Category of System: | IT System If “other” is selected, please describe: Click here to enter text. |



Homeland Security

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

Privacy Threshold Analysis
Version number: 01-2014
Page 9 of 10

| | |
|--|---|
| <p>Determination:</p> <ul style="list-style-type: none"> <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: | <p>System covered by existing PIA</p> <p>If covered by existing PIA, please list: DHS/CBP/PIA-006(b) Automated Targeting System (ATS) DHS/CBP/PIA-007(g) Electronic System for Travel Authorization (ESTA)</p> |
| SORN: | <p>System covered by existing SORN</p> <p>If covered by existing SORN, please list: DHS/CBP-006 Automated Targeting System, May 22, 2012, 77 FR 30297 DHS/CBP-009 Electronic System for Travel Authorization, September 2, 2016, 81 FR 60713</p> |
| <p>DHS Privacy Office Comments: Please describe rationale for privacy compliance determination above.</p> | |
| <p>CBP is submitting this PTA to discuss the next update for the ESTA Social Media Pilot. This update involves use of a new social media vetting tool. (b) (7)(E)</p> <div style="background-color: black; color: white; text-align: center; padding: 20px; font-size: 2em; font-weight: bold;">(b) (7)(E)</div> | |
| <p>The DHS Privacy Office finds this initiative privacy-sensitive.</p> <p>Coverage is provided by DHS/CBP/PIA-007 ESTA and the DHS/CBP-009 ESTA. The Privacy Office agrees that coverage for this pilot is also provided under DHS/CBP/PIA-006 ATS, which outlines CBP's use of decision support tools in order to compare traveler information against law enforcement, intelligence, and other enforcement data. Additionally, this PIA outlines the querying of publicly available information in support of the vetting process. The DHS Privacy Office also agrees that SORN coverage is provided by the DHS/CBP-006 ATS SORN, which notes that CBP collects information on</p> | |



**Homeland
Security**

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

Privacy Threshold Analysis

Version number: 01-2014

Page 10 of 10

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

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