

Order No.	Vendor Name	Smart Number (PIID)	CLIN	Short Text Description	Pgr Branch	Pgr Div	Order Qty	OU	Effective Date	Current End Date	End Date w/Opts	PSC/FS	Fund	Funds center	Funds Ctr Title	Functional Area	Matl Group	Other Agency/Referenced IDV	PO Count	Order No.	Contract Type
119514144	TROPHOLZ TECHNOLOGIES, INC	70804C18F0000377		(b) (7)(E)	(b) (7)(E)	(b) (7)(E)		EA	(b) (7)(E)			7030	(b) (7)(E)	(b) (7)(E)	(b) (7)(E)	(b) (7)(E)			1	2000	FFP
			10	(b) (7)(E)													315B				
166669742	PANAMERICA COMPUTERS, INC.	70804C18F00001093		(b) (7)(E)				EA				7050					315B		1	2000	FFP
			10	(b) (7)(E)				EA									315B				
			20	(b) (7)(E)				EA									315B			2000	
119514144	TROPHOLZ TECHNOLOGIES, INC	70804C18F00001257		(b) (7)(E)				EA				7030					315B		1	2000	FFP
			10	(b) (7)(E)				EA									315B				
			20	(b) (7)(E)				EA									315B			2000	
			30	(b) (7)(E)				EA									315B			2000	
			40	(b) (7)(E)				EA									2525			2000	
			50	(b) (7)(E)				EA									315B			2000	
			60	(b) (7)(E)				EA									2525			2000	
603814054	GOVERNMENT ACQUISITIONS INC	H5BP1008123674		(b) (7)(E)				EA				7025					315B		1	2000	FFP
			110	(b) (7)(E)													315B				
181194650	NING INC	H5BP1010P00746							8/16/2010	2/27/2012	2/27/2012	D309							1	2000	FFP
			10				1	AU									2525			2000	
			20				1	AU									2525			2000	
825732746	FEDERAL BUSINESS COUNCIL INC	H5BP1012F00119		(b) (7)(E)				AU	(b) (7)(E)			R408					2525	(b) (7)(E)	1	2000	FFP
			60	(b) (7)(E)				AU	(b) (7)(E)								2525				
88365767	CARASOFT TECHNOLOGY CORP	H5BP1014P00537						AU	8/15/2014	8/14/2015	8/14/2015	R426							1	2000	FFP
			10				1	AU									2515				
809887164	THUNDERCAT TECHNOLOGY LLC	H5BP1015J00880		(b) (7)(E)				EA	(b) (7)(E)			D319					315B		1	2000	FFP
			10	(b) (7)(E)				EA	(b) (7)(E)								315B			2000	
			20	(b) (7)(E)				EA	(b) (7)(E)								315B			2000	
809887164	THUNDERCAT TECHNOLOGY LLC	H5BP1016J00747		(b) (7)(E)				EA				D319					315B		1	2000	FFP
			10	(b) (7)(E)													315B				
809887164	THUNDERCAT TECHNOLOGY LLC	H5BP1017J00831		(b) (7)(E)				EA				7030					315B		1	2000	FFP
			10	(b) (7)(E)				EA									315B			2000	
			20	(b) (7)(E)				EA									315B			2000	
			30	(b) (7)(E)				EA									315B			2000	

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 08/15/2014	2. CONTRACT NO. (if any)	6. SHIP TO:			
3. ORDER NO. HSBP1014P00537	4. REQUISITION/REFERENCE NO. 0020079578	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
		f. SHIP VIA			
7. TO:		8. TYPE OF ORDER			
a. NAME OF CONTRACTOR CARAHSOFT TECHNOLOGY CORP		<input checked="" 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 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 12369 SUNRISE VALLEY DR STE D2					
d. CITY RESTON	e. STATE VA	f. ZIP CODE 20191		10. REQUISITIONING OFFICE (b) (6), (b) (7)(C)	
9. ACCOUNTING AND APPROPRIATION DATA					

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 WOMEN-OWNED SMALL BUSINESS 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) 08/15/2014	16. DISCOUNT TERMS Net 30
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)	Acct
10	Social Media Monitoring Service	1.000	AU	(b) (7)(C)	(b) (7)(E)	

SEE BILLING INSTRUCTIONS REVERSE	18. SHIPPING POINT	19. GROSS SHIPPING WEIGHT	20. INVOICE NO.		\$0.00	17(h)TOT (Cont. pages)	
	21. MAIL INVOICE TO:						
	a. NAME DHS - Customs & Border Protection		Commercial Accounts Sect.			\$38,315.00	17(i) GRAND TOTAL
	b. STREET ADDRESS (or P.O. Box) 6650 Telecom Drive, Suite 100						
c. CITY Indianapolis		d. STATE IN	e. ZIP CODE 46278				

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

AUTHORIZED FOR LOCAL REPRODUCTION
Previous edition not usable

OPTIONAL FORM 347 (REV. 5/2011)
Prescribed by GSA/FAR 48 CFR 53.213 (f)

NOTES:

Purchase Order HSBP1014P00537 in the amount of \$38,315.00 is to be awarded to Carahsoft for social media monitoring services. The period of performance is 1 year after receipt of order (ARO).

Please see the Statement of Work (SOW) for all requirements under this order.

Program Office Contact:

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

For contract related questions, please contact the Contract Specialist:

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

Attachments:

1. Accounting Data and Terms and Conditions
2. Statement of Work
3. Quote

PURCHASE ORDER TERMS AND CONDITIONS

U.S. CUSTOMS and BORDER PROTECTION

Supplemental Clauses/Provisions

Order Number: HSBP1014P00537

I.1 SCHEDULE OF SUPPLIES/SERVICES

ITEM #	DESCRIPTION	QTY	UNIT	UNIT PRICE	EXT. PRICE
10	Social Media Monitoring Service	1.000	AU	(b) (4)	(b) (4)

Total Funded Value of Award:

\$38,315.00

I.2 ACCOUNTING and APPROPRIATION DATA

ITEM #	ACCOUNTING and APPROPRIATION DATA	AMOUNT
10	(b) (7)(E)	(b) (4)

I.3 DELIVERY SCHEDULE

DELIVER TO:	ITEM #	QTY	DELIVERY DATE
DHS - Customs & Border Protection Office:Commissioner Sit Room & IMOC 1300 Pennsylvania Ave NW Rm7.2A Washington, DC 20229	10	1.000	(b) (7)(E)

II.1 52.252-2 CLAUSES INCORPORATED BY REFERENCE (FEB 1998)

This contract incorporates one or more clauses by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. Also, the full text of a clause may be accessed electronically at this/these address(es):
www.acquisition.gov

I. FEDERAL ACQUISITION REGULATION (48 CHAPTER 1) CLAUSES

NUMBER TITLE

II.2 52.204-13 SYSTEM FOR AWARD MANAGEMENT MAINTENANCE (JUL 2013)

II.3 52.212-4 CONTRACT TERMS AND CONDITIONS--COMMERCIAL ITEMS (MAY 2014)

II.4 52.212-5 CONTRACT TERMS AND CONDITIONS REQUIRED TO IMPLEMENT STATUTES OR EXECUTIVE ORDERS--COMMERCIAL ITEMS (JUL 2014)

(a) The Contractor shall comply with the following Federal Acquisition Regulation (FAR) clauses, which are incorporated in this contract by reference, to implement provisions of law or Executive orders applicable to acquisitions of commercial items:

(1) 52.222-50, Combating Trafficking in Persons (FEB 2009) (22 U.S.C. 7104(g)).

Alternate I (AUG 2007) of 52.222-50 (22 U.S.C. 7104(g)).

(2) 52.233-3, Protest After Award (AUG 1996) (31 U.S.C. 3553).

(3) 52.233-4, Applicable Law for Breach of Contract Claim (OCT 2004) (Public Laws 108-77 and 108-78 (19 U.S.C. 3805 note)).

(b) The Contractor shall comply with the FAR clauses in this paragraph (b) that the Contracting Officer has indicated as being incorporated in this contract by reference to implement provisions of law or Executive orders applicable to acquisitions of commercial items:

[Contracting Officer check as appropriate]

(1) 52.203-6, Restrictions on Subcontractor Sales to the Government (SEP 2006), with Alternate I (OCT 1995) (41 U.S.C. 4704 and 10 U.S.C. 2402).

(2) 52.203-13, Contractor Code of Business Ethics and Conduct (APR 2010) (41 U.S.C. 3509).

(3) 52.203-15, Whistleblower Protections Under the American Recovery and Reinvestment Act of 2009 (JUN 2010) (Section 1553 of Pub. L. 111-5). Applies to contracts funded by the American Recovery and Reinvestment Act of 2009.)

(4) 52.204-10, Reporting Executive Compensation and First-Tier Subcontract Awards (JUL 2013) (Pub. L. 109-282) (31 U.S.C. 6101 note).

(5) [Reserved]

(6) 52.204-14, Service Contract Reporting Requirements (JAN 2014) (Pub. L. 111-117, section 743 of Div. C).

- (7) 52.204-15, Service Contract Reporting Requirements for Indefinite-Delivery Contracts (JAN 2014) (Pub. L. 111-117, section 743 of Div. C).
- (8) 52.209-6, Protecting the Government's Interest When Subcontracting with Contractors Debarred, Suspended, or Proposed for Debarment (AUG 2013) (31 U.S.C. 6101 note).
- (9) 52.209-9, Updates of Publicly Available Information Regarding Responsibility Matters (JUL 2013) (41 U.S.C. 2313)
- (10) 52.209-10, Prohibition on Contracting with Inverted Domestic Corporations (MAY 2012) (section 738 of Division C of Pub. L. 112-74, section 740 of Division C of Pub. L. 111-117, section 743 of Division D of Pub. L. 111-8, and section 745 of Division D of Pub. L. 110-161).
- (11) 52.219-3, Notice of HUBZone Set-Aside or Sole-Source Award (NOV 2011) (15 U.S.C. 657a).
- (12) 52.219-4, Notice of Price Evaluation Preference for HUBZone Small Business Concerns (JAN 2011) (if the offeror elects to waive the preference, it shall so indicate in its offer) (15 U.S.C. 657a).
- (13) [Reserved]
- (14) (i) 52.219-6, Notice of Total Small Business Set-Aside (NOV 2011) (15 U.S.C. 644).
 - (ii) Alternate I (NOV 2011).
 - (iii) Alternate II (NOV 2011).
- (15) (i) 52.219-7, Notice of Partial Small Business Set-Aside (JUN 2003) (15 U.S.C. 644).
 - (ii) Alternate I (OCT 1995) of 52.219-7.
 - (iii) Alternate II (MAR 2004) of 52.219-7.
- (16) 52.219-8, Utilization of Small Business Concerns (MAY 2014) (15 U.S.C. 637(d)(2) and (3)).
- (17) (i) 52.219-9, Small Business Subcontracting Plan (JUL 2013) (15 U.S.C. 637(d)(4)).
 - (ii) Alternate I (OCT 2001) of 52.219-9.
 - (iii) Alternate II (OCT 2001) of 52.219-9.
 - (iv) Alternate III (JUL 2010) of 52.219-9.
- (18) 52.219-13, Notice of Set-Aside of Orders (NOV 2011) (15 U.S.C. 644(r)).
- (19) 52.219-14, Limitations on Subcontracting (NOV 2011) (15 U.S.C. 637(a)(14)).
- (20) 52.219-16, Liquidated Damages--Subcontracting Plan (JAN 1999) (15 U.S.C. 637(d)(4)(F)(i)).
- (21)(i) 52.219-23, Notice of Price Evaluation Adjustment for Small Disadvantaged Business Concerns (OCT 2008) (10 U.S.C. 2323) (if the offeror elects to waive the adjustment, it shall so indicate in its offer).
 - (ii) Alternate I (JUN 2003) of 52.219-23.
- (22) 52.219-25, Small Disadvantaged Business Participation Program--Disadvantaged Status and Reporting (JUL 2013) (Pub. L. 103-355, section 7102, and 10 U.S.C. 2323).

- [] (23) 52.219-26, Small Disadvantaged Business Participation Program--Incentive Subcontracting (OCT 2000) (Pub. L. 103-355, section 7102, and 10 U.S.C. 2323).
- [] (24) 52.219-27, Notice of Service-Disabled Veteran-Owned Small Business Set-Aside (NOV 2011) (15 U.S.C. 657f).
- [] (25) 52.219-28, Post Award Small Business Program Rerepresentation (JUL 2013) (15 U.S.C. 632(a)(2)).
- [] (26) 52.219-29, Notice of Set-Aside for Economically Disadvantaged Women-Owned Small Business (EDWOSB) Concerns (JUL 2013) (15 U.S.C. 637(m)).
- [] (27) 52.219-30, Notice of Set-Aside for Women-Owned Small Business (WOSB) Concerns Eligible Under the WOSB Program (JUL 2013) (15 U.S.C. 637(m)).
- [] (28) 52.222-3, Convict Labor (JUN 2003) (E.O. 11755).
- [] (29) 52.222-19, Child Labor--Cooperation with Authorities and Remedies (JAN 2014) (E.O. 13126).
- [] (30) 52.222-21, Prohibition of Segregated Facilities (FEB 1999).
- [] (31) 52.222-26, Equal Opportunity (MAR 2007) (E.O. 11246).
- [] (32) 52.222-35, Equal Opportunity for Veterans (JUL 2014) (38 U.S.C. 4212).
- [] (33) 52.222-36, Affirmative Action for Workers with Disabilities (JUL 2014) (29 U.S.C. 793).
- [] (34) 52.222-37, Employment Reports on Veterans (JUL 2014) (38 U.S.C. 4212).
- [] (35) 52.222-40, Notification of Employee Rights Under the National Labor Relations Act (DEC 2010) (E.O. 13496).
- [] (36) 52.222-54, Employment Eligibility Verification (AUG 2013). (Executive Order 12989). (Not applicable to the acquisition of commercially available off-the-shelf items or certain other types of commercial items as prescribed in 22.1803.)
- [] (37)(i) 52.223-9, Estimate of Percentage of Recovered Material Content for EPA-Designated Products Items (MAY 2008) (42 U.S.C. 6962(c)(3)(A)(ii)). (Not applicable to the acquisition of commercially available off-the-shelf items.)
 - [] (ii) Alternate I (MAY 2008) of 52.223-9 (42 U.S.C. 6962(i)(2)(C)). (Not applicable to the acquisition of commercially available off-the-shelf items.)
- [] (38) (i) 52.223-13, Acquisition of EPEAT®-Registered Imaging Equipment (JUN 2014) (E.O.s 13423 and 13514).
 - [] (ii) Alternate I (JUN 2014) of 52.223-13.
- [] (39) (i) 52.223-14, Acquisition of EPEAT®-Registered Televisions (JUN 2014) (E.O.s 13423 and 13514).
 - [] (ii) Alternate I (JUN 2014) of 52.223-14.
- [] (40) 52.223-15, Energy Efficiency in Energy--Consuming Products (DEC 2007) (42 U.S.C. 8259b).

- (41)(i) 52.223-16, Acquisition of EPEAT®-Registered Personal Computer Products (JUN 2014) (E.O.s 13423 and 13514).
 - (ii) Alternate I (JUN 2014) of 52.223-16.
- (42) 52.223-18, Encouraging Contractor Policies to Ban Text Messaging While Driving (AUG 2011).
- (43) 52.225-1, Buy American—Supplies (MAY 2014) (41 U.S.C. chapter 83).
- (44)(i) 52.225-3, Buy American—Free Trade Agreements—Israeli Trade Act (MAY 2014) (41 U.S.C. chapter 83, 19 U.S.C. 3301 note, 19 U.S.C. 2112 note, 19 U.S.C. 3805 note, 19 U.S.C. 4001 note, Pub. L. 103–182, 108–77, 108–78, 108–286, 108–302, 109–53, 109–169, 109–283, 110–138, 112–41, 112–42, and 112–43).
 - (ii) Alternate I (MAY 2014) of 52.225-3.
 - (iii) Alternate II (MAY 2014) of 52.225-3.
 - (iv) Alternate III (MAY 2014) of 52.225-3.
- (45) 52.225-5, Trade Agreements (NOV 2013) (19 U.S.C. 2501, et seq., 19 U.S.C. 3301 note).
- (46) 52.225-13, Restrictions on Certain Foreign Purchases (JUN 2008) (E.o.s, proclamations, and statutes administered by the Office of Foreign Assets Control of the Department of the Treasury).
- (47) 52.225-26, Contractors Performing Private Security Functions Outside the United States (JUL 2013) (Section 862, as amended, of the National Defense Authorization Act for Fiscal Year 2008; 10 U.S.C. 2302 Note).
- (48) 52.226-4, Notice of Disaster or Emergency Area set-Aside (NOV 2007)
- (49) 52.226-5, Restrictions on Subcontracting Outside Disaster or Emergency Area (NOV 2007)
- (50) 52.232-29, Terms for Financing of Purchases of Commercial Items (FEB 2002) (41 U.S.C. 4505, 10 U.S.C. 2307(f)).
- (51) 52.232-30, Installment Payments for Commercial Items (OCT 1995) (41 U.S.C. 4505, 10 U.S.C. 2307(f)).
- (52) 52.232-33, Payment by Electronic Funds Transfer--System for Award Management (JUL 2013) (31 U.S.C. 3332).
- (53) 52.232-34, Payment by Electronic Funds Transfer--Other than System for Award Management (JUL 2013) (31 U.S.C. 3332).
- (54) 52.232-36, Payment by Third Party (MAY 2014) (31 U.S.C. 3332).
- (55) 52.239-1, Privacy or Security Safeguards (AUG 1996) (5 U.S.C. 552a).
- (56)(i) 52.247-64, Preference for Privately Owned U.S.-Flag Commercial Vessels (FEB 2006) (46 U.S.C. Appx. 1241(b) and 10 U.S.C. 2631).
 - (ii) Alternate I (APR 2003) of 52.247-64.

(c) The Contractor shall comply with the FAR clauses in this paragraph (c), applicable to commercial services, that the Contracting Officer has indicated as being incorporated in this contract by reference to implement provisions of law or Executive orders applicable to acquisitions of commercial items: [Contracting Officer check as appropriate.]

(1) 52.222-41, Service Contract Labor Standards (MAY 2014) (41 U.S.C. chapter 67).

(2) 52.222-42, Statement of Equivalent Rates for Federal Hires (MAY 2014) (29 U.S.C. 206 and 41 U.S.C. chapter 67).

(3) 52.222-43, Fair Labor Standards Act and Service Contract Labor Standards—Price Adjustment (Multiple Year and Option Contracts) (MAY 2014) (29 U.S.C. 206 and 41 U.S.C. chapter 67).

(4) 52.222-44, Fair Labor Standards Act and Service Contract Labor Standards—Price Adjustment (MAY 2014) (29 U.S.C. 206 and 41 U.S.C. chapter 67).

(5) 52.222-51, Exemption from Application of the Service Contract Labor Standards to Contracts for Maintenance, Calibration, or Repair of Certain Equipment—Requirements (MAY 2014) (41 U.S.C. Chapter 67).

(6) 52.222-53, Exemption from Application of the Service Contract Labor Standards to Contracts for Certain Services—Requirements (MAY 2014) (41 U.S.C. chapter 67).

(7) 52.222-17, Nondisplacement of Qualified Workers (MAY 2014) (E.O. 13495).

(8) 52.226-6, Promoting Excess Food Donation to Nonprofit Organizations (MAY 2014) (42 U.S.C. 1792).

(9) 52.237-11, Accepting and Dispensing of \$1 Coin (SEP 2008) (31 U.S.C. 5112(p)(1)).

(d) Comptroller General Examination of Record The Contractor shall comply with the provisions of this paragraph (d) if this contract was awarded using other than sealed bid, is in excess of the simplified acquisition threshold, and does not contain the clause at 52.215-2, Audit and Records--Negotiation.

(1) The Comptroller General of the United States, or an authorized representative of the Comptroller General, shall have access to and right to examine any of the Contractor's directly pertinent records involving transactions related to this contract.

(2) The Contractor shall make available at its offices at all reasonable times the records, materials, and other evidence for examination, audit, or reproduction, until 3 years after final payment under this contract or for any shorter period specified in FAR Subpart 4.7, Contractor Records Retention, of the other clauses of this contract. If this contract is completely or partially terminated, the records relating to the work terminated shall be made available for 3 years after any resulting final termination settlement. Records relating to appeals under the disputes clause or to litigation or the settlement of claims arising under or relating to this contract shall be made available until such appeals, litigation, or claims are finally resolved.

(3) As used in this clause, records include books, documents, accounting procedures and practices, and other data, regardless of type and regardless of form. This does not require the Contractor to create or maintain any record that the Contractor does not maintain in the ordinary course of business or pursuant to a provision of law.

(e) (1) Notwithstanding the requirements of the clauses in paragraphs (a), (b), (c), and (d) of this clause, the Contractor is not required to flow down any FAR clause, other than those in paragraphs (e)(1) in a subcontract for commercial items. Unless otherwise indicated below, the extent of the flow down shall be as required by the clause--

- (i) 52.203-13, Contractor Code of Business Ethics and Conduct (APR 2010) (41 U.S.C. 3509).
 - (ii) 52.219-8, Utilization of Small Business Concerns (MAY 2014) (15 U.S.C. 637(d)(2) and (3)), in all subcontracts that offer further subcontracting opportunities. If the subcontract (except subcontracts to small business concerns) exceeds \$650,000 (\$1.5 million for construction of any public facility), the subcontractor must include 52.219-8 in lower tier subcontracts that offer subcontracting opportunities.
 - (iii) 52.222-17, Nondisplacement of Qualified Workers (MAY 2014) (E.O. 13495). Flow down required in accordance with paragraph (l) of FAR clause 52.222-17.
 - (iv) 52.222-26, Equal Opportunity (MAR 2007) (E.O. 11246).
 - (v) 52.222-35, Equal Opportunity for Veterans (JUL 2014) (38 U.S.C. 4212).
 - (vi) 52.222-36, Affirmative Action for Workers with Disabilities (JUL 2014) (29 U.S.C. 793).
 - (vii) 52.222-37, Employment Reports on Veterans (JUL 2014) (38 U.S.C. 4212)
 - (viii) 52.222-40, Notification of Employee Rights Under the National Labor Relations Act (DEC 2010) (E.O. 13496). Flow down required in accordance with paragraph (f) of FAR clause 52.222-40.
 - (ix) 52.222-41, Service Contract Labor Standards (MAY 2014) (41 U.S.C. chapter 67).
 - (x) 52.222-50, Combating Trafficking in Persons (FEB 2009) (22 U.S.C. 7104(g)).
 - Alternate I (AUG 2007) of 52.222-50 (22 U.S.C. 7104(g)).
 - (xi) 52.222-51, Exemption from Application of the Service Contract Labor Standards to Contracts for Maintenance, Calibration, or Repair of Certain Equipment—Requirements (MAY 2014) (41 U.S.C. chapter 67).
 - (xii) 52.222-53, Exemption from Application of the Service Contract Labor Standards to Contracts for Certain Services—Requirements (MAY 2014) (41 U.S.C. chapter 67).
 - (xiii) 52.222-54, Employment Eligibility Verification (AUG 2013).
 - (xiv) 52.225-26, Contractors Performing Private Security Functions Outside the United States (JUL 2013) (Section 862, as amended, of the National Defense Authorization Act for Fiscal Year 2008; 10 U.S.C. 2302 Note).
 - (xv) 52.226-6, Promoting Excess Food Donation to Nonprofit Organizations (MAY 2014) (42 U.S.C. 1792). Flow down required in accordance with paragraph (e) of FAR clause 52.226-6.
 - (xvi) 52.247-64, Preference for Privately Owned U.S.-Flag Commercial Vessels (FEB 2006) (46 U.S.C. Appx 1241(b) and 10 U.S.C. 2631). Flow down required in accordance with paragraph (d) of FAR clause 52.247-64.
- (2) While not required, the contractor may include in its subcontracts for commercial items a minimal number of additional clauses necessary to satisfy its contractual obligations.

(End of clause)

II.5 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)

II.6 52.232-99 PROVIDING ACCELERATED PAYMENT TO SMALL BUSINESS SUBCONTRACTORS (DEVIATION)

This clause implements the temporary policy provided by OMB Policy Memorandum *M-12-16, Providing Prompt Payment to Small Business Subcontractors*, dated July 11, 2012.

- (a) Upon receipt of accelerated payments from the Government, the contractor is required to make accelerated payments to small business subcontractors to the maximum extent practicable after receipt of a proper invoice and all proper documentation from the small business subcontractor.
- (b) Include the substance of this clause, including this paragraph (b), in all subcontracts with small business concerns.
- (c) The acceleration of payments under this clause does not provide any new rights under the Prompt Payment Act.

(End of clause)

II.7 TERM OF CONTRACT (MARCH 2003)

The term of this contract is 1 year after receipt of order (ARO).

[End of Clause]

II.8 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]

II.9 PAYMENT AND INVOICE INSTRUCTIONS (APR 2014)

In order to request contract payment, the contractor shall submit a proper invoice, as defined by Federal Acquisition Regulation (FAR) 2.101 for payment in the manner and format described below.

SUBMISSION OF INVOICES

- (a) The contractor shall submit an original invoice/voucher, via postal mail or electronic mail (email), simultaneously to the following:

- (1) U.S. Customs and Border Protection
Commercial Accounts Section
6650 Telecom Drive, Suite 100
Indianapolis, Indiana 46278

OR email: cbpinvoices@dhs.gov

NOTE: For invoices with payment terms less than net 30, the subject line for all emailed invoices must include the following text: "**Per CBP, Net [state # days] Invoice**".

- (2) Contracting Officer or Contract Administrator (CO)

DHS/U.S. Customs and Border Protection
Attention: (b) (6), (b) (7)(C)

OR email: (b) (6), (b) (7)(C)

- (3) Contracting Officer's Representative (COR)

DHS/U.S. Customs and Border Protection
Attention: (b) (6), (b) (7)(C)

OR email: (b) (6), (b) (7)(C)

- (b) The contractor shall submit a copy of the original invoice/voucher for all DHS cost-reimbursement and time and material/labor hour contracts and delivery orders to the branch manager/resident auditor of the cognizant Defense Contract Audit Agency (DCAA) Field Audit Office. Copies may be sent to DCAA, via postal mail or email and must be sent at the same time the invoice/voucher is sent to the NFC, CO and COR. The CO shall provide the following information:

DCAA Field Office
Attention:

Phone:

Email:

- (c) 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.

INVOICE 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).
- (2) For cost reimbursement or time and material contracts (other than a contract for a commercial item), the contractor shall bill and maintain a record of indirect costs in accordance with FAR 52.216-7(d).
- (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.

ADDITIONAL INVOICE REQUIREMENTS

In addition to the invoice requirements contained in FAR 32.905 and FAR 52.216-7, the following also applies:

- (1) Invoices must include the following information to support all costs claimed:
 - i. Period of performance for the costs claimed;
 - ii. Current amounts for each CLIN, if applicable;
 - iii. Current direct and indirect incurred costs, including fee;
 - iv. Cumulative amounts for each CLIN; and
 - v. Statement signed by an authorized company representative certifying that the costs in the invoice are accurate and complete.
- (2) The Government reserves the right to make invoice adjustments if associated costs are determined to be unallowable.

[End of Clause]

II.10 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]

II.11 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]

II.12 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]

Statement of Work (SOW)

1. PROJECT TITLE: To provide the (b) (7)(E) analysts the capability to (b) (7)(E)

2. BACKGROUND: (b) (5), (b) (7)(E)

The (b) mission continues to grow ever more complex with new initiatives, data, and interaction between CBP and stakeholders around the world. When National Security events take place, it is crucial that the (b) (7)(E)

As part of this initiative, the (b) (7)(E)

3. SCOPE: This Statement of Work (SOW) covers the request to (b) (7)(E)

(b) (7)(E) assigned to or employed by Customs and Border Protection are considered (b) (7)(E)

(b) (7)(E)

The work required will be performed in a commercial off the shelf (COTS) manner.

- (b) (7)(E)
- The service shall provide information from (b) (7)(E)
- Ensure the employees of the company providing the service (b) (7)(E)
- CBP request (b) (7)(E)
- Training class and materials for (b) (7)(E), (b) (5)

4. **APPLICABLE DOCUMENTS:** CBP is mandated by legislation, and executive order to purchase products that are good for the environment. To the extent possible, all equipment should conform to the Energy Star Program, Federal Energy Management Program (FEMP), Electronic Product Environmental Assessment Tool (EPEAT), and other Federal environmentally preferable programs as specified in the Federal Acquisition Regulations (FAR) Part 23.

SPECIFIC TASKS:

- (b) (7)(E)
- (b) (7)(E)
- Ensure data integrity
- Automated link-analysis
- (b) (7)(E)
- Inform CBP when the data or the monitoring service has been compromised

5. **DELIVERABLES AND DELIVERY SCHEDULE:** Monthly Progress Report - *Social Media Monitoring Service* Contractor shall provide a written monthly status report that provides the technical and financial status of all ongoing work performed under the contract. Summaries of meetings shall also be included in the monthly report. Receipt of this report is due by the 25th calendar day of each subsequent month if applicable. Contractor format is acceptable but must be approved by the COTR. At a minimum an individual copy will be provided to the *Social Media Monitoring Service* program manager and the COTR. Contents shall include:

- * Status of project and all tasks in progress. Problems encountered (technical/schedule/cost) should be identified and resolutions noted. Unresolved problems/issues should be highlighted at the end of the reporting period.
- * Identification of current and cumulative expenditures for both hours and dollars, noting the amount by account that is funded and computation of the remaining account balances.
- * Identification of the names of all individuals charging against the purchase order. Data should be organized by contract labor category and document both current and cumulative hours charged for each person (when applicable).

Other Summary Reports - Upon request of the government, *Social Media Monitoring Service* Contractor shall provide oral and written reports and summaries on:

- integration and employment of complex analytic methodologies necessary to meet operational mission requirements (when applicable);
- operations, maintenance, training and documentation support associated with

implementation of the deployed system (when applicable);

- program plans and schedules documenting work associated with the purchase order completion (when applicable);

- documentation and tracking of any meetings and configuration control activities (when applicable);

- memorandum for the record documenting the details, discussions, and actions items of contractor and government meeting shall be provided for all meetings where programmatic, technical and implementation strategies are discussed.

Training - *Social Media Monitoring Service* Contractor shall provide instructors, course preparation, on-site and classroom instruction and curriculum development and maintenance. *Social Media Monitoring Service* Contractor shall provide hard copies and electronic copies of all training presentations and/or materials in a format and on media as specified. Updated and revised user manuals and operations and maintenance support documents and release notes in accordance with government release management requirements for major releases shall be provided as directed by the COTR.

Social Media Monitoring Service shall provide at least two references of other government customers receiving the same or similar service.

6. GOVERNMENT-FURNISHED EQUIPMENT AND INFORMATION: No Government-Furnished equipment will be provided for this acquisition.
7. PLACE OF PERFORMANCE: Performance will be carried out through delivery of service. No on-site service is required.
8. PERIOD OF PERFORMANCE: Performance will be carried out through delivery of service. The contracted service term shall one year after receipt of order (ARO).

Social Media Monitoring Service Deliverable Schedule

ITEMS	No. of copies and Format	Due date After Award
Monthly Progress Report	Electronic	25 th of each month for the Social Media Monitoring Service COR
Summary Reports	Electronic	As required in the purchase order for the COR
Training Material	One Hard Copy And Electronic copy	As required in the purchase order

9. **SECURITY:** Work will not be carried out on-site and will not require a security classification level.

**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) software.

(b) (7)(E) must have the ability to analyze social media in order to gain further insight in accurately identifying and organizing groups of people based on social media postings. The (b) (7)(E) web-based application is a multi-lingual, geo-enabled, text-analytics open source intelligence (OSINT) platform which was developed to meet the specialized needs of law enforcement and their intelligence organizations. The (b) (7)(E) platform (b) (7)(E) by persistently monitoring and analyzing open-source, third party, and client-owned data sources through advanced statistical, linguistic, and crowd sourcing techniques.

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

2.0 Period of Performance

The period of performance for this contract will be 9/21/17-9/20/18.

This is a 12 month period of performance.

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. The primary location for this work is below. Travel to other Washington DC area Government locations may be necessary.

- a. (b) (7)(E) Kingstowne Facility, 5971 Kingstowne Village Parkway, Alexandria, VA 22315

4.0 Deliverables

The contractor shall provide the following deliverables:

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

5.0 Type of Contract

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

6.0 Point of Contact

CONTRACTING OFFICER’S REPRESENTATIVE

Name: (b) (6), (b) (7)(C)
 Address:
 Tel. #:
 Fax. #:
 Email:

CONTRACTING OFFICER’S REPRESENTATIVE – ALTERNATE

Name: (b) (6), (b) (7)(C)
 Address:
 Tel. #:
 Fax. #:
 Email:

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.

7.0 Clauses

The Contractor shall fulfill the duties of this SOW while maintaining full compliance with all terms and conditions of the contract. Please see below for IT security and agency specific clauses applicable to this contract.

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).

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 COR 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 COR. 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. 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 COR 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 COR 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 COR 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. 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 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.

OAST (Office on Accessible Systems and Technology) Compliance

Accessibility Requirements (Section 508)

Section 508 of the Rehabilitation Act, as amended by the Workforce Investment Act of 1998 (P.L. 105-220) requires that when Federal agencies develop, procure, maintain, or use electronic and information technology (EIT), they must ensure that it is accessible to people with disabilities. Federal employees and members of the public who have disabilities must have equal access to and use of information and data that is comparable to that enjoyed by non-disabled Federal employees and members of the public.

All EIT deliverables within this work statement shall comply with the applicable technical and functional performance criteria of Section 508 unless exempt. Specifically, the following applicable EIT accessibility standards have been identified:

Section 508 Applicable EIT Accessibility Standards

36 CFR 1194.21 Software Applications and Operating Systems, applies to all EIT software applications and operating systems procured or developed under this work statement including but not limited to GOTS and COTS software. In addition, this standard is to be applied to Web-based applications when needed to fulfill the functional performance criteria. This standard also applies to some Web based applications as described within 36 CFR 1194.22.

36 CFR 1194.22 Web-based Intranet and Internet Information and Applications, applies to all Web-based deliverables, including documentation and reports procured or developed under this work statement. When any Web application uses a dynamic (non-static) interface, embeds custom user control(s), embeds video or multimedia, uses proprietary or technical approaches such as, but not limited to, Flash or Asynchronous Javascript and XML (AJAX) then 1194.21 Software standards also apply to fulfill functional performance criteria.

36 CFR 1194.31 Functional Performance Criteria, applies to all EIT deliverables regardless of delivery method. All EIT deliverable shall use technical standards, regardless of technology, to fulfill the functional performance criteria.

36 CFR 1194.41 Information Documentation and Support, applies to all documents, reports, as well as help and support services. To ensure that documents and reports fulfill the required 1194.31 Functional Performance Criteria, they shall comply with the technical standard associated with Web-based Intranet and Internet Information and Applications at a minimum. In addition, any help or support provided in this work statement that offer telephone support, such as, but not limited to, a help desk shall have the ability to transmit and receive messages using TTY.

Section 508 Applicable Exceptions

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 COR and determination will be made in accordance with DHS MD 4010.2. DHS has identified the following exceptions that may apply: 36 CFR 1194.3(b) Incidental to Contract, all EIT that is exclusively owned and used by the contractor to fulfill this work statement does not require compliance with Section 508. This exception does not apply to any EIT deliverable, service or item that will be used by any Federal employee(s) or member(s) of the public. This exception only applies to those contractors assigned to fulfill the obligations of this work statement and for the purposes of this requirement, are not considered members of the public.

Section 508 Compliance Requirements

36 CFR 1194.2(b) (COTS/GOTS products), When procuring a product, each agency shall procure products which comply with the provisions in this part when such products are available in the commercial marketplace or when such products are developed in response to a Government solicitation. Agencies cannot claim a product as a whole is not commercially available because no product in the marketplace meets all the standards. If products are commercially available that meet some but not all of the standards, the agency must procure the product that best meets the standards. When applying this standard, all procurements of EIT shall have documentation of market research that identify a list of products or services that first meet the agency business needs, and from that list of products or services, an analysis that the selected product met more of the accessibility requirements than the non-selected products as required by FAR 39.2. 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) in accordance with DHS MD 4010.2.

All tasks for testing of functional and/or technical requirements must include specific testing for Section 508 compliance, and must use DHS Office of Accessible Systems and Technology approved testing methods and tools. For information about approved testing methods and tools send an email to accessibility@dhs.gov.

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.

System Security documentation appropriate for the SELC status.

Security Certification/Accreditation

CBP Program Offices shall provide personnel (System Owner and Information System Security Officers) with the appropriate clearance levels to support the security certification/accreditation processes under this Agreement in accordance with the current version of the DHS MD 4300A, DHS Sensitive Systems Policy and Handbook, CBP Information Systems Security Policies and Procedures Handbook HB-1400-05, and all applicable National Institute of Standards and Technology (NIST) Special Publications (800 Series). During all SELC phases of CBP systems, CBP personnel shall develop documentation and provide any required information for all levels of classification in support of the certification/accreditation process. In addition, all security certification/accreditation will be performed using the DHS certification/accreditation process, methodology and tools. An ISSO performs security actions for an information system. There is only one ISSO designated to a system, but multiple Alternate ISSOs may be designated to assist the ISSO. While the ISSO performs security functions, the System Owner is always responsible for information system security (4300A). System owners shall include information security requirements in their capital planning and investment control (CPIC) business cases for the current budget year and for the Future Years Homeland Security Program (FYHSP) for each DHS information system. System owners or AOs shall ensure that information security requirements and POA&Ms are adequately funded, resourced and documented in accordance with current OMB budgetary guidance.

Disaster Recovery Planning & Testing – Hardware

If the system owner requires a robust DR solution (full redundancy and failover capabilities (for near zero downtime)) then the funded DR solution must match the production environment like-for-like. This solution would also include additional software licenses, hardware, firmware and storage for the DR environment.

The system owner or program office must also include travel, per diem and approximately 16 over the core hours for travel to recovery facilities twice per fiscal year for system administrators, DBA's, end users or testers

If the system owner requires a moderate DR solution that would provide a working environment that is capable of handling their mission essential functions then they can fund a scaled down

solution which should still take into consideration additional hardware, software licenses, and storage for the DR environment.

The system owner or program office is still responsible for the costs associated with testing their DR solution; however, for a scaled down solution, it may be possible to leverage or share staff already designated to participate in DR activities.

If the system owner only requires a low DR solution then the system owner or program office can use internal resources to perform a table-top exercise, which generally does not require travel, additional hardware or software licenses.

Monitoring/reviewing contractor security requirements clause

Security Review and Reporting

(a) The Contractor shall include security as an integral element in the management of this contract. The Contractor shall conduct reviews and report the status of the implementation and enforcement of the security requirements contained in this contract and identified references.

(b) The Government may elect to conduct periodic reviews to ensure that the security requirements contained in this contract are being implemented and enforced. The Contractor shall afford DHS including the organization of the DHS Office of the Chief Information Officer, Office of Inspector General, the CBP Chief Information Security Officer, authorized Contracting Officer's Technical Representative (COR), and other government oversight organizations, access to the Contractor's and subcontractors' facilities, installations, operations, documentation, databases, and personnel used in the performance of this contract. The Contractor will contact the DHS Chief Information Security Officer to coordinate and participate in the review and inspection activity of government oversight organizations external to the DHS. Access shall be provided to the extent necessary for the government to carry out a program of inspection, investigation, and audit to safeguard against threats and hazards to the integrity, availability, and confidentiality of DHS/CBP data or the function of computer systems operated on behalf of DHS/CBP, and to preserve evidence of computer crime.

Access to Unclassified Facilities, Information Technology Resources, and Sensitive Information

The assurance of the security of unclassified facilities, Information Technology (IT) resources, and sensitive information during the acquisition process and contract performance are essential to the DHS mission. DHS Management Directive (MD) 11042.1 *Safeguarding Sensitive But Unclassified (For Official Use Only) Information*, describes how contractors must handle sensitive but unclassified information. DHS MD 4300.1 *Information Technology Systems Security* and the *DHS Sensitive Systems Handbook* prescribe policies and procedures on security for IT resources. Contractors shall comply with these policies and procedures, any replacement publications, or any other current or future DHS policies and procedures covering contractors specifically for all Task Orders that require access to DHS facilities, IT resources or sensitive information. Contractors shall not use or redistribute any DHS information processed, stored, or transmitted by the contractor except as specified in the task order.

OMB-M-07-18 FDCC

In acquiring information technology, agencies shall include the appropriate information technology security policies and requirements, including use of common security configurations available from the National Institute of Standards and Technology's website at <http://checklists.nist.gov>. Agency contracting officers should consult with the requiring official to ensure the appropriate standards are incorporated.

Engineering Platforms

Common Enterprise Services (CES) – Deliver the systems, infrastructure, and operational capabilities to fully implement the three service levels defined as part of the DHS/CBP Common Enterprise Services and support DHS Component use of those services. This includes the build out and integration of all required services and infrastructure, which must include the Single Sign-on Portal and CBP Enterprise Services Bus (ESB), required for the CES. Capabilities shall be designed to the DHS standard operating architecture (SOA), transportable between DHS data centers (CBP National Data Center, Stennis, and DHS 2nd data center).

Single Sign-on Portal – Design, build, and operate a single sign-on Portal - consistent with DHS' enterprise portal solution (for which ICE is the steward) - to provide a common point of access, with a single sign-on capability to existing applications and to provide the infrastructure for integrating diverse internal and/or external information and transactional resources. This includes the migration of the current ACE Portal to the Single Sign-on Portal as rapidly as feasible.

ITP (Infrastructure Transformation Program) COMPLIANCE

Help Desk and Operations Support

The contractor shall provide third tier reporting for trouble calls received from the Help Desk, the DHS Task Manager, or the users. The Contractor shall respond to the initiators of trouble calls as by receiving telephonic notifications of problems, resolving them, or directing them to the proper technical personnel for resolution. Problems that cannot be resolved immediately or with the requirements of the performance standards are to be brought to the attention of the DHS Task Manager. The Contractor shall document notification and resolution of problems in Remedy.

Interfacing

As requested by the COR, assistance in consolidating all systems with the DHS Consolidated Data Center. Resources to be consolidated with the DHS Consolidated Data Center for each system to be determined by the COR.

TRANSITION PLAN

The DHS CIO has established portfolio targets for the IT infrastructure that include production system consolidation at a DHS data center, and transition to OneNet. The contractor must be prepared to support CBP government leads, within the purview of this task order, to provide any required transition planning or program execution, associated with meeting the agreed to transition timeline, as directed by Government personnel. This includes the following types of taskings:

- Coordination with Government representatives
- Review, evaluation and transition of current support services
- Transition of historic data to new contractor system
- Government-approved training and certification process
- Transfer of all necessary business and/or technical documentation
- Orientation phase and program to introduce Government personnel, programs, and users to the Contractor's team, tools, methodologies, and business processes, equipment, furniture, phone lines, computer equipment, etc.
- Transfer of Government Furnished Equipment (GFE) and Government Furnished Information (GFI), and GFE inventory management assistance
- Applicable debriefing and personnel out-processing procedures

Portfolio Review

Screening/Watchlist/Credentialing

Includes all activities that support the tracking and monitoring of travelers, conveyances and cargo crossing U.S. borders, and traffic pattern analysis, database (Federal, State, and Local) linking and querying, and managing status verification and tracking systems. Different investments and systems may support distinct screening and watchlist activities for people, cargo, and tangible goods. Credentialing encompasses all activities that determine a person's eligibility for a particular license, privilege, or status, from application for the credential through issuance, use, and potential revocation of the issued credential.



PRIVACY THRESHOLD ANALYSIS (PTA)

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

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

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

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

PIA@hq.dhs.gov

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

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



PRIVACY THRESHOLD ANALYSIS (PTA)

SUMMARY INFORMATION

Project or Program Name:	(b) (4), (b) (7)(E)		
Component:	Customs and Border Protection (CBP)	Office or Program:	Office of Information Technology/Cyber Security Directorate
Xacta FISMA Name	(b) (4), (b) (7)(E)	Xacta FISMA Number	(b) (7)(E)
Type of Project or Program:	IT System	Project or program status:	Development
Date first developed:		Pilot launch date:	June 29, 2018
Date of last PTA update	N/A	Pilot end date:	N/A
ATO Status (if applicable)	In progress	ATO expiration date (if applicable):	Pending

BUSINESS OWNER/ GOVERNMENT USER

Name:	(b) (6), (b) (7)(C)		
Office:	OIT/CSD	Title:	Executive Director Cyber Security Directorate/ CBP CISO
Phone:	(b) (6), (b) (7)(C)	Email:	(b) (6), (b) (7)(C)

PROJECT OR PROGRAM MANAGER

Name:	(b) (6), (b) (7)(C)		
Office:	OIT/CSD	Title:	Project Manager
Phone:	(b) (6), (b) (7)(C)	Email:	(b) (6), (b) (7)(C)

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)



Specific PTA Questions

1. Reason for submitting the PTA: New PTA

U.S. Customs and Border Protection (CBP) is submitting this new PTA for (b) (4), (b) (7)(E) (b) (4), (b) (7)(E) which enables authorized CBP personnel with an operational need to safely (b) (7)(E) (b) (7)(E) Some CBP employees may need access to perform (b) (7)(E) that involve

(b) (7)(E)

Background

The (b) (7)(E) is a DHS-wide solution to provide authorized DHS personnel with (b) (7)(E)

(b) (7)(E)

Effective June 30th, 2018, (b) (7)(E) is no longer supported by DHS. To ensure CBP authorized personnel (b) (7)(E)

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

Overview

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

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



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

The **(b) (4), (b) (7)(E)** users will need to adhere to CBP's Social Media Policy and the relevant Social Media Operational Use Templates (SMOUTs) and complete the appropriate Privacy and Rules of Behavior Training prior to receiving a **(b) (4), (b) (7)(E)** account.

(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 type="checkbox"/> Social Media</p> <p><input type="checkbox"/> Web portal¹ (e.g., SharePoint)</p> <p><input type="checkbox"/> Contact Lists</p> <p><input checked="" type="checkbox"/> None of these</p>
---	--

<p>3. From whom does the Project or Program collect, maintain, use, or disseminate information?</p>	<p><input type="checkbox"/> This program does not collect any personally identifiable information²</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.



<i>Please check all that apply.</i>	<input checked="" type="checkbox"/> Members of the public <input checked="" type="checkbox"/> DHS employees/contractors (list components): CBP <input checked="" type="checkbox"/> Contractors working on behalf of DHS <input type="checkbox"/> Employees of other federal agencies
-------------------------------------	--

4. What specific information about individuals is collected, generated or retained?

The following information is collected and retained on CBP ^{(b) (4), (b) (7)(E)} users:

- Work Email
- Work Station ID
- First Name
- Last Name

In addition to CBP ^{(b) (4), (b) (7)(E)} user account information, a variety of information obtained by ^{(b) (7)(E)}

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

4(a) Does the project, program, or system retrieve information by personal identifier?	<input type="checkbox"/> No. Please continue to next question. <input checked="" type="checkbox"/> Yes. Work Email, Work Station ID, First Name, and Last Name
4(b) Does the project, program, or system use Social Security Numbers (SSN)?	<input checked="" type="checkbox"/> No. <input type="checkbox"/> Yes.
4(c) If yes, please provide the specific legal basis and purpose for the collection of SSNs:	N/A
4(d) If yes, please describe the uses of the SSNs within the project, program, or system:	N/A
4(e) If this project, program, or system is an information technology/system, does it relate solely to infrastructure?	<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.



For example, is the system a Local Area Network (LAN) or Wide Area Network (WAN)?	
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 checked="" type="checkbox"/> No. <input type="checkbox"/> Yes. If yes, please list: Click here to enter text.
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: Click here to enter text.
6(a) Is this external sharing pursuant to new or existing information sharing access agreement (MOU, MOA, LOI, etc.)?	Choose an item. 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. Yes. Mandatory social media privacy training is provided, as well as operational training on the use of social media.
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?	<input type="checkbox"/> No. What steps will be taken to develop and maintain the accounting: <input checked="" type="checkbox"/> Yes. CBP routinely shares information with other DHS components, Federal law enforcement, other government agencies (OGA) and elements of the Intelligence Community, on an as needed basis (in the event derogatory is identified). CBP will

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.



	maintain record of this exchange via email (often at the classified level). Disclosures made to individuals who request access to their own PII are managed through the FOIA/Privacy Act process.
9. 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: Confidentiality: <input type="checkbox"/> Low <input checked="" type="checkbox"/> Moderate <input type="checkbox"/> High <input type="checkbox"/> Undefined Integrity: <input type="checkbox"/> Low <input checked="" type="checkbox"/> Moderate <input type="checkbox"/> High <input type="checkbox"/> Undefined Availability: <input type="checkbox"/> Low <input checked="" 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:	August 15, 2018
Date submitted to DHS Privacy Office:	September 25, 2018
Component Privacy Office Recommendation: <i>Please include recommendation below, including what new privacy compliance documentation is needed.</i>	
(b) (5), (b) (7)(E)	

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.



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

[Redacted text block containing multiple paragraphs and bulleted items]



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

[Redacted content]

- [Redacted content]
- [Redacted content]
- [Redacted content]
- [Redacted content]

(TO BE COMPLETED BY THE DHS PRIVACY OFFICE)

DHS Privacy Office Reviewer:	(b) (6), (b) (7)(C)
PCTS Workflow Number:	(b) (7)(E)
Date approved by DHS Privacy Office:	October 10, 2018
PTA Expiration Date	October 10, 2021

DESIGNATION

Privacy Sensitive System:	Yes If "no" PTA adjudication is complete.
Category of System:	IT System



If "other" is selected, please describe: Click here to enter text.	
Determination:	<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 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:	Choose an item. If covered by existing PIA, please list: Click here to enter text.
SORN:	System covered by existing SORN If covered by existing SORN, please list: DHS/ALL-004 General Information Technology Access Account Records System (GITAARS) SORN, November 27, 2012, 77 FR 70792
DHS Privacy Office Comments:	
<i>Please describe rationale for privacy compliance determination above.</i>	
CBP is submitting this new PTA for (b) (4), (b) (7)(E) which enables authorized CBP personnel with an operational need to (b) (7)(E)	
<div style="background-color: black; color: white; padding: 20px; font-size: 2em; font-weight: bold;">(b) (7)(E)</div>	
<div style="background-color: black; color: white; padding: 20px; font-size: 2em; font-weight: bold;">(b) (4), (b) (7)(E)</div>	



Privacy Threshold Analysis

Version number: 01-2014

Page 11 of 11

The DHS Privacy Office finds that the (b) (4), (b) (7)(E) users will need to adhere to CBP's Social Media Policy and the relevant SMOUTs and complete the appropriate Privacy and Rules of Behavior Training prior to receiving a (b) (4), (b) (7)(E) account.

(b) (4), (b) (7)(E) is privacy sensitive and therefore PIA and SORN coverage is required.

PRIV agrees with CBP Privacy that (b) (4), (b) (7)(E) is an HR-only system and does not require a PIA because PII is collected from only CBP-employees to gain access. SORN coverage is provided by DHS/ALL-004, which covers Business contact information used to access IT resources, such as (b) (4), (b) (7)(E) (b) (4), (b) (7)(E)

Work papers and products generated by CBP employees while using (b) (4), (b) (7)(E) are covered by the following PIAs and SORNs:

- DHS/CBP/PIA-010 Analytical Framework for Intelligence System (AFI);
- DHS/CBP/PIA-006 Automated Targeting System;
- DHS/CBP/PIA-009(a) TECS System: CBP Primary and Secondary Processing (TECS) National SAR Initiative;
- DHS/CBP/PIA-021 TECS System: Platform;
- DHS/CBP/PIA-012 CBP Portal (E3) to ENFORCE/IDENT;
- DHS/CBP/PIA-039 CBP Situation Room;
- DHS/CBP/PIA-044 Joint Integrity Case Management System (JICMS);
- DHS/CBP-017 Analytical Framework for Intelligence System (AFI), June 7, 2012 77 FR 13813;
- DHS/CBP 024 Intelligence Records System (CIRS) System of Records, September 21, 2017, 82 FR 44198;
- DHS/CBP-006 Automated Targeting System, May 22, 2012, 77 FR 30297;
- DHS/CBP-011 U.S. Customs and Border Protection TECS, December 19, 2008, 73 FR 77778;
- DHS/CBP-023 Border Patrol Enforcement Records (BPER), October 20, 2016, 81 FR 72601; and
- DHS/ALL-020 Department of Homeland Security Internal Affairs April 28, 2014, 79 FR 23361.



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



PRIVACY THRESHOLD ANALYSIS (PTA) SUMMARY INFORMATION

Project or Program Name:	ESTA Social Media Tool Pilot Evaluation		
Component:	CBP	Office or Program:	OFO (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)

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)



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)



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)

2. Does this system employ any of the following technologies:

If you are using any of these technologies and want coverage under the respective PIA for that technology please stop here and contact the DHS Privacy Office for further guidance.

- Closed Circuit Television (CCTV)
- Social Media
- Web portal¹ (e.g., SharePoint)
- Contact Lists
- None of these

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.



<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.



<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. 	
4(a) Does the project, program, or system retrieve information by personal identifier?	<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) <div style="background-color: black; width: 100px; height: 1em; margin-top: 5px;"></div>
4(b) Does the project, program, or system use Social Security Numbers (SSN)?	<input checked="" type="checkbox"/> No. <input type="checkbox"/> Yes.
4(c) If yes, please provide the specific legal basis and purpose for the collection of SSNs:	N/A
4(d) If yes, please describe the uses of the SSNs within the project, program, or system:	N/A
4(e) If this project, program, or system is an information technology/system, does it relate solely to infrastructure? <i>For example, is the system a Local Area Network (LAN) or Wide Area Network (WAN)?</i>	<input checked="" type="checkbox"/> No. Please continue to next question. <input type="checkbox"/> Yes. If a log kept of communication traffic, please answer the following question.



4(f) If header or payload 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.



<p>individuals/agencies who have requested access to their PII?</p>	<p>(b) (4), (b) (7)(E)</p> <p><input type="checkbox"/> Yes. In what format is the accounting maintained:</p>
<p>9. Is there a FIPS 199 determination?⁵</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:</p> <p><input type="checkbox"/> Low <input checked="" type="checkbox"/> Moderate <input type="checkbox"/> High <input type="checkbox"/> Undefined</p> <p>Integrity:</p> <p><input checked="" type="checkbox"/> Low <input type="checkbox"/> Moderate <input type="checkbox"/> High <input type="checkbox"/> Undefined</p> <p>Availability:</p> <p><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:	June 21, 2016
Date submitted to DHS Privacy Office:	July 7, 2016
<p>Component Privacy Office Recommendation:</p> <p><i>Please include recommendation below, including what new privacy compliance documentation is needed.</i></p>	
<p>(b) (5), (b) (7)(E)</p> <p>[Redacted]</p> <p>[Redacted]</p> <p>[Redacted]</p> <p>[Redacted]</p> <p>[Redacted]</p> <p>[Redacted]</p>	

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.



(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



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>_____</p> <p>_____</p> <p>_____</p> <p>_____</p> <p>_____</p> <p>_____</p> <p>_____</p> <p>_____</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>	



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 text block containing multiple lines of blacked-out information]



PRIVACY THRESHOLD ANALYSIS (PTA)

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

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

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

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

PIA@hq.dhs.gov

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

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



PRIVACY THRESHOLD ANALYSIS (PTA)

SUMMARY INFORMATION

Project or Program Name:	ESTA Social Media Tool Pilot Evaluation, Update 1		
Component:	Customs and Border Protection (CBP)	Office or Program:	OFO (b) (7))
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	July 29, 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)		
Office:	OFO	Title:	Director
Phone:	(b) (6), (b) (7)(C)	Email:	(b) (6), (b) (7)(C)

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)



SPECIFIC PTA QUESTIONS

1. Reason for submitting the PTA: Updated PTA

CBP ESTA Social Media Vetting is a pilot project. As a pilot, vetting activities will expand and contract based on new information identified and new areas of interest. This PTA is Update 1 to the ESTA Social Media Tool Pilot Evaluation PTA, adjudicated July 8, 2016.

In an effort to test the capabilities of the social media vetting tools, S&T and CBP seek to look at cases

(b) (7)(E)

1. ESTA Cases Approved for a Waiver

a.

b.

c.

d.

(b) (7)(E)

2. Automatically Approved by the ESTA Online System

a.

b.

c.

(b) (7)(E)

2. Does this system employ any of the following technologies:

If you are using any of these technologies and want coverage under the respective PIA for that technology please stop here and contact the DHS Privacy Office for further guidance.

- Closed Circuit Television (CCTV)
- Social Media



- Internet protocol (IP) address;
- ESTA application number;
- Country of residence;

New Data being evaluated:

(b) (7)(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: All ESTA application fields may be searched by the tool.</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.



<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:</p> <p>PII for ESTA applications is provided by CBP (b) (7)(E) to S&T to facilitate the pilot. (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:</p> <p>(b) (4), (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</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:</p> <p>(b) (4), (b) (7)(E)</p>

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.



	<input type="checkbox"/> Yes. In what format is the accounting maintained:
9. 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: 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:	July 29, 2016
Date submitted to DHS Privacy Office:	August 2, 2016
Component Privacy Office Recommendation: <i>Please include recommendation below, including what new privacy compliance documentation is needed.</i>	
(b) (5), (b) (7)(E) _____ _____ _____ _____	

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.



(b) (5)

■ [Redacted]

■ [Redacted]

(TO BE COMPLETED BY THE DHS PRIVACY OFFICE)

DHS Privacy Office Reviewer:	(b) (6), (b) (7)(C)
PCTS Workflow Number:	(b) (7)(E)
Date approved by DHS Privacy Office:	August 19, 2016
PTA Expiration Date	December 31, 2017 or the end of this pilot, whichever comes first.

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(b) Automated Targeting System (ATS) Update, June 1, 2012
SORN:	System covered by existing SORN If covered by existing SORN, please list: DHS/CBP-006 - Automated Targeting System May 22, 2012, 77 FR 30297
DHS Privacy Office Comments: <i>Please describe rationale for privacy compliance determination above.</i>	
CBP and S&T are expanding the ESTA social media pilot to include (b) (7)(E) (b) (7)(E) PRIV finds that this pilot continues to receive coverage under the ATS PIA and SORN. (b) (5)	
[Redacted]	
[Redacted]	
[Redacted]	
[Redacted]	



PRIVACY THRESHOLD ANALYSIS (PTA)

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

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

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

Senior Director, Privacy Compliance
The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
Tel: 202 (b) (7)(E)

(b) (7)(E)@hq.dhs.gov

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

A copy of the Guide and Template is available on the DHS Privacy Office website, www.dhs.gov/privacy, on DHSConnect and directly from the DHS Privacy Office via email:

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



PRIVACY THRESHOLD ANALYSIS (PTA)

SUMMARY INFORMATION

Project or Program Name:	ESTA Social Media Tool Pilot Evaluation, Update 2		
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	July 29, 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)		
Office:	OFO	Title:	Director
Phone:	(b) (6), (b) (7)(C)	Email:	(b) (6), (b) (7)(C)

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)



SPECIFIC PTA QUESTIONS

1. Reason for submitting the PTA: Updated PTA

CBP ESTA Social Media Vetting is a pilot project. As a pilot, vetting activities will be fluid to allow for a range of information to be researched. This PTA is Update 2 to the ESTA Social Media Tool Pilot Evaluation PTA, adjudicated July 8, 2016.

The ESTA pilot (June 11th – September 9th) showed potential to (b) (7)(E) (b) (7)(E) This PTA update supports transition of the pilot-developed methodology into CBP's (b) (7)(E) (b) (7)(E). S&T and CBP seek to look at visa waiver cases that CBP may review in carrying out its daily mission:

1. ESTA Cases Being Considered for a Waiver

- a. (b) (7)(E)
- b. (b) (7)(E)
- c. (b) (7)(E)
- d. (b) (7)(E)

2. ESTA Cases already Automatically Approved by the ESTA Online System

- a. (b) (7)(E)
- b. (b) (7)(E)
- c. (b) (7)(E)
- b. (b) (7)(E)
-) (b) (7)(E)

This update also includes piloting of new tools, in addition to (b) (4), (b) (7)(E) which has been used to-date. S&T continues to test open source and social media tools for the Department. 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) (4), (b) (7)(E)



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

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

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

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

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



(b) (4), (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. 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. 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.



4. What specific information about individuals is collected, generated or retained?

(b) (7)(E)

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).

The full list of ESTA application fields is below (Stated in the July 8, 2016 PTA and updated to reflect the request for applicants' social media accounts, if approved):

- 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

New Data being evaluated:

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

<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 may be searched by the tool.</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>



4(d) If yes, please describe the uses of the SSNs within the project, program, or system:	Click here to enter text.
4(e) If this project, program, or system is an information technology/system, does it relate solely to infrastructure? <i>For example, is the system a Local Area Network (LAN) or Wide Area Network (WAN)?</i>	<input checked="" type="checkbox"/> No. Please continue to next question. <input type="checkbox"/> Yes. If a log kept of communication traffic, please answer the following question.
4(f) If header or payload data³ 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: 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. For the operational pilot, (b) (7)(E) However, these tools will not be connected to DHS systems.
6. Does this project, program, or system connect, receive, or share PII with any external (non-DHS) partners or systems?	<input type="checkbox"/> No. <input checked="" type="checkbox"/> Yes. If yes, please list: (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.



	(b) (4), (b) (7)(E)
6(a) Is this external sharing pursuant to new or existing information sharing access agreement (MOU, MOA, LOI, etc.)?	Existing Please describe applicable information sharing governance in place:
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 individuals/agencies who have requested access to their PII?	<input checked="" type="checkbox"/> No. What steps will be taken to develop and maintain the accounting: (b) (4), (b) (7)(E) <input type="checkbox"/> Yes. In what format is the accounting maintained:
9. 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: 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:

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.



(b) (5)

(TO BE COMPLETED BY THE DHS PRIVACY OFFICE)

DHS Privacy Office Reviewer:	(b) (6), (b) (7)(C)
PCTS Workflow Number:	(b) (7)(E)
Date approved by DHS Privacy Office:	November 21, 2016
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:	System covered by existing PIA If covered by existing PIA, please list: DHS/CBP/PIA-006(b) Automated Targeting System (ATS) DHS/CBP/PIA-007(g) Electronic System for Travel Authorization (ESTA)
SORN:	System covered by existing SORN If covered by existing SORN, please list: DHS/CBP-006 Automated Targeting System, May 22, 2012, 77 FR 30297



	DHS/CBP-009 Electronic System for Travel Authorization, September 2, 2016, 81 FR 60713
DHS Privacy Office Comments: <i>Please describe rationale for privacy compliance determination above.</i>	
CBP is submitting this PTA to (b) (5) [REDACTED]	
<p>The collection of ESTA applicant information is covered by the DHS/CBP/PIA-007(g) ESTA and the DHS/CBP-009 ESTA SORN, which was recently updated to include social media identifiers, such as username(s) and platforms used.</p> <p>The Privacy Office agrees that coverage for this pilot is provided under DHS/CBP/PIA-006(b) 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>(b) (5) [REDACTED]</p>	



PRIVACY THRESHOLD ANALYSIS (PTA)

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

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

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

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

PIA@hq.dhs.gov

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

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



PRIVACY THRESHOLD ANALYSIS (PTA)

SUMMARY INFORMATION

Project or Program Name:	ESTA Social Media Tool Pilot Evaluation, Update 2		
Component:	Science and Technology (S&T)	Office or Program:	HSARPA
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	July 29, 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)		
Office:	HSARPA	Title:	Director, DA-E
Phone:	(b) (6), (b) (7)(C)	Email:	(b) (6), (b) (7)(C)

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)



SPECIFIC PTA QUESTIONS

1. Reason for submitting the PTA: Updated PTA

This update includes piloting of new tools, in addition to (b) (4), (b) (7)(E) which has been used to-date. S&T continues to test open source and social media tools for the Department. 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) (4), (b) (7)(E)

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

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

(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>
---	--

<p>3. From whom does the Project or Program collect, maintain, use, or disseminate information?</p>	<p><input type="checkbox"/> This program does not collect any personally identifiable information²</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.



<i>Please check all that apply.</i>	<input checked="" type="checkbox"/> Members of the public <input type="checkbox"/> DHS employees/contractors (list components): <input type="checkbox"/> Contractors working on behalf of DHS <input type="checkbox"/> Employees of other federal agencies
-------------------------------------	---

4. What specific information about individuals is collected, generated or retained?
<p>The Social Media tools are being tested using ESTA data.</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 (Stated in the July 8, 2016 PTA and updated to reflect the request for applicants' social media accounts, if approved):</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>New Data being evaluated:</p> <p style="text-align: center; font-size: 2em;">(b) (7)(E)</p>



4(a) Does the project, program, or system retrieve information by personal identifier?	<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 may be searched by the tool.
4(b) Does the project, program, or system use Social Security Numbers (SSN)?	<input checked="" type="checkbox"/> No. <input type="checkbox"/> Yes.
4(c) If yes, please provide the specific legal basis and purpose for the collection of SSNs:	Click here to enter text.
4(d) If yes, please describe the uses of the SSNs within the project, program, or system:	Click here to enter text.
4(e) If this project, program, or system is an information technology/system, does it relate solely to infrastructure? <i>For example, is the system a Local Area Network (LAN) or Wide Area Network (WAN)?</i>	<input checked="" type="checkbox"/> No. Please continue to next question. <input type="checkbox"/> Yes. If a log kept of communication traffic, please answer the following question.
4(f) If header or payload data³ 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: 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. (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.



	For the operational pilot, (b) (7)(E) (b) (7)(E)
6. Does this project, program, or system connect, receive, or share PII with any external (non-DHS) partners or systems?	<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.)?	Existing 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 individuals/agencies who have requested access to their PII?	<input checked="" type="checkbox"/> No. What steps will be taken to develop and maintain the accounting: (b) (4), (b) (7)(E) <input type="checkbox"/> Yes. In what format is the accounting maintained:
9. Is there a FIPS 199 determination? ⁴	<input type="checkbox"/> Unknown.

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.



	<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:	July 29, 2016
Date submitted to DHS Privacy Office:	November 15, 2016
Component Privacy Office Recommendation: <i>Please include recommendation below, including what new privacy compliance documentation is needed.</i>	
(b) (5)	
[Redacted]	
[Redacted]	
[Redacted]	
[Redacted]	
[Redacted]	



(b) (5)

[Redacted content]

(TO BE COMPLETED BY THE DHS PRIVACY OFFICE)

DHS Privacy Office Reviewer:	(b) (6), (b) (7)(C)
PCTS Workflow Number:	(b) (7)(E)
Date approved by DHS Privacy Office:	November 21, 2016
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:	New PIA is required. If covered by existing PIA, please list: New Social Media Vetting PIA
-------------	--

SORN:	System covered by existing SORN If covered by existing SORN, please list: DHS/S&T-001 Research, Development, Test, and Evaluation Records, January 15, 2013, 78 FR 3019
--------------	--

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

S&T is submitting the PTA to discuss the piloting of new tools, in addition to (b) (4), (b) (7)(E) which has been used to-date. (b) (5)

PRIV finds that is a privacy sensitive system and a PIA is required because S&T collects PII from members of the public.

(b) (5) Social Media Vetting PIA will discuss the social media tools developed by S&T as well as the limited amount of social media data collected and used to (b) (7)(E)

PRIV finds that a SORN is required because S&T (b) (7)(E) S&T has said it will use CBP data for test and evaluation only, therefore, PRIV agrees with S&T that the Research, Development, Test, and Evaluation SORN adequately provides coverage. DHS/S&T-001 covers records that are collected for the purpose of furthering S&T's mission to push innovation and development, and the use of high technology in support of homeland security.

This phase of this pilot may include other social media tools. (b) (5)

(b) (5) This PTA expires at the end of the pilot on December 31, 2017.



**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.



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)

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)



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)



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.

2. Does this system employ any of the following technologies:

If you are using any of these technologies and want coverage under the respective PIA for that technology please stop here and contact the DHS Privacy Office for further guidance.

- Closed Circuit Television (CCTV)
- Social Media
- Web portal¹ (e.g., SharePoint)
- Contact Lists
- None of these

3. From whom does the Project or Program collect, maintain, use, or disseminate information?

Please check all that apply.

- This program does not collect any personally identifiable information²
- Members of the public
- DHS employees/contractors (list components):
- Contractors working on behalf of DHS
- Employees of other federal agencies

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.



4. What specific information about individuals is collected, generated or retained?

(b) (7)(E)

[REDACTED]. As part of this pilot, CBP will also collect publicly available information from social media platforms to 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] 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)

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)



<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) (2) 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.



	<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:</p> <p>Information from ESTA applications is (b) (7)(E)</p> <p>(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:</p> <p>CBP and S&T are disclosing information to vendors</p> <p>(b) (4), (b) (7)(E)</p> <p>The other vendors will be treated accordingly when a contract or CRADA is in place.</p>



	<p>(b) (4), (b) (7)(E)</p> <p><input type="checkbox"/> Yes. In what format is the accounting maintained:</p>
<p>8. Is there a FIPS 199 determination?⁴</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: (The reference is for S&T's Data Analytics laboratory, which brings in many tools for evaluation for various projects.)</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)
------------------------------------	----------------------------

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

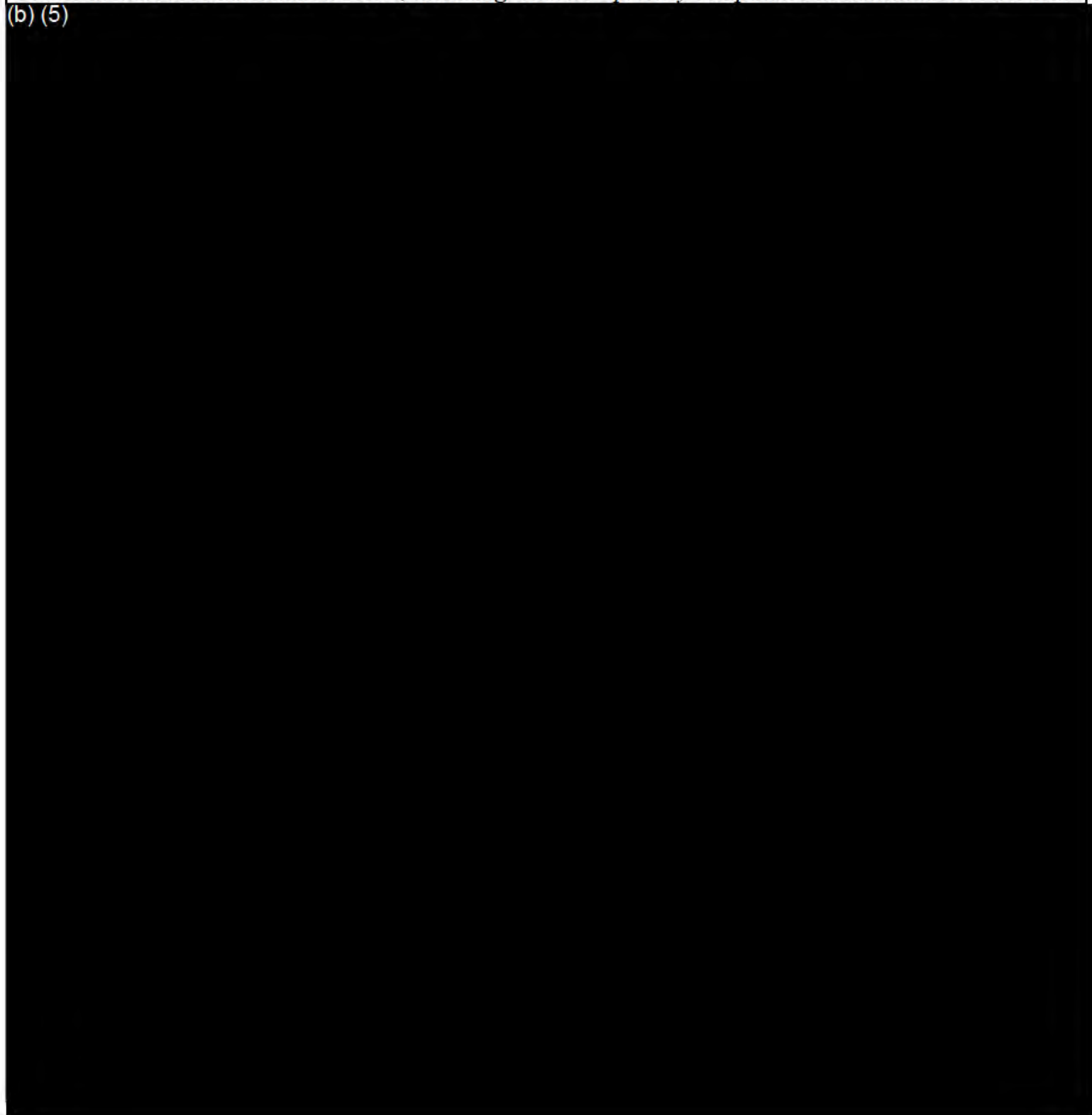
Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
202-343-1717, pia@dhs.gov
www.dhs.gov/privacy

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)





(TO BE COMPLETED BY THE DHS PRIVACY OFFICE)

DHS Privacy Office Reviewer:	(b) (6), (b) (7)(C)
PCTS Workflow Number:	(b) (7)(E)
Date approved by DHS Privacy Office:	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: [REDACTED] 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:



	DHS/CBP-006 Automated Targeting System, May 22, 2012, 77 FR 30297 DHS/CBP-009 Electronic System for Travel Authorization, September 2, 2016, 81 FR 60713
--	---

DHS Privacy Office Comments:

Please describe rationale for privacy compliance determination above.

CBP is submitting this PTA to discuss the next update for the ESTA Social Media Pilot. 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.

The DHS Privacy Office finds that this phase of the pilot is privacy-sensitive, requiring both PIA and SORN coverage.

(b) (7)(E) 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.

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.

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.

This PTA expires with the pilot end date on December 31, 2017. The S&T privacy compliance documentation requirements do not impede pilot operations.



PRIVACY THRESHOLD ANALYSIS (PTA)

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

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

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

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

PIA@hq.dhs.gov

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

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



PRIVACY THRESHOLD ANALYSIS (PTA)

SUMMARY INFORMATION

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

PROJECT OR PROGRAM MANAGER

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

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)



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

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

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

a. (b) (7)(E)

b. (b) (7)(E)

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



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

<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>
--	--

<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 assist in assessing the eligibility of ESTA applicants to travel under Visa Waiver Program (VWP). Any derogatory information collected from social media and deemed operationally relevant will be stored in ATS-TF.</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.



<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.



<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) (4), (b) (7)(E) (b) (4), (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) (4), (b) (7)(E) (b) (4), (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) (4), (b) (7)(E)</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:</p> <p>(b) (4), (b) (7)(E)</p> <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.



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:	(b) (7)(E)
Date approved by DHS Privacy Office:	January 5, 2018
PTA Expiration Date	January 5, 2021

DESIGNATION

Privacy Sensitive System:	Yes If "no" PTA adjudication is complete.
Category of System:	IT System If "other" is selected, please describe: Click here to enter text.



Determination:	
<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(b) Automated Targeting System (ATS) DHS/CBP/PIA-007(g) Electronic System for Travel Authorization (ESTA)
SORN:	System covered by existing SORN If covered by existing SORN, please list: DHS/CBP-006 Automated Targeting System, May 22, 2012, 77 FR 30297 DHS/CBP-009 Electronic System for Travel Authorization, September 2, 2016, 81 FR 60713
DHS Privacy Office Comments:	
<i>Please describe rationale for privacy compliance determination above.</i>	
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) (4), (b) (7)(E)	
<div style="background-color: black; color: white; padding: 10px; font-size: 2em; font-weight: bold;">(b) (4), (b) (7)(E)</div>	
The DHS Privacy Office finds this initiative privacy-sensitive. Coverage is provided by DHS/CBP/PIA-007 ESTA and the DHS/CBP-009 ESTA. The Privacy Office agrees that coverage for this pilot is also provided under DHS/CBP/PIA-006 ATS, which outlines CBP's use of decision support tools in order to compare traveler information against law enforcement, intelligence, and other enforcement data. Additionally, this PIA outlines the querying of publicly available information in support of the vetting process. The DHS Privacy Office also agrees that SORN coverage is provided by the DHS/CBP-006 ATS SORN, which notes that CBP collects information on	



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.