SOLICITATION/CONTRACT/ORDER FOR COMMERCIAL ITEMS
OFFEROR TO COMPLETE BLOCKS 12, 17, 23, 24, & 30

1. REQUISITION NUMBER	PAGE	OF
HCT190124	1	30

2. CONTRACT NO.	3. AWARD/ EFFECTIVE DATE	4. ORDER NUMBER	5. SOLICITATION NUMBER	6. SOLICITATION ISSUE DATE
	09/30/2019	70SBUR19P00000128	70SBUR19Q00000313	09/11/2019

7. FOR SOLICITATION INFORMATION CALL:	a. NAME	b. TELEPHONE NUMBER (No collect calls)	8. OFFER DUE DATE/LOCAL TIME
	BLAKE EMERY	802-872-4595	

9. ISSUED BY — CODE: CIS

USCIS Contracting Office
Department of Homeland Security
70 Kimball Avenue
South Burlington VT 05403

10. THIS ACQUISITION IS
- ☐ UNRESTRICTED OR ☒ SET ASIDE: 100.00 % FOR:
- ☒ SMALL BUSINESS
- ☐ HUBZONE SMALL BUSINESS
- ☐ SERVICE-DISABLED VETERAN-OWNED SMALL BUSINESS
- ☐ WOMEN-OWNED SMALL BUSINESS (WOSB) ELIGIBLE UNDER THE WOMEN-OWNED SMALL BUSINESS PROGRAM
- ☐ EDWOSB
- ☐ 8(A)

NAICS: 541611
SIZE STANDARD: $16.5

11. DELIVERY FOR FOB DESTINATION UNLESS BLOCK IS MARKED	12. DISCOUNT TERMS	13a. THIS CONTRACT IS A RATED ORDER UNDER DPAS (15 CFR 700)	13b. RATING	14. METHOD OF SOLICITATION
☒ SEE SCHEDULE	Net 30	☐		☒ RFQ ☐ IFB ☐ RFP

15. DELIVER TO — CODE: HCT

HUMAN CAPITAL AND TRAINING OFFICE
70 Kimball Avenue
So. Burlington VT 05403

16. ADMINISTERED BY — CODE: CIS

USCIS Contracting Office
Department of Homeland Security
70 Kimball Avenue
South Burlington VT 05403

17a. CONTRACTOR/ OFFEROR — CODE: 8274311280000 — FACILITY CODE:

GUARDIAN DEFENSE GROUP LLC
8647 RICHMOND HIGHWAY
648
ALEXANDRIA VA 22309

TELEPHONE NO.

☐ 17b. CHECK IF REMITTANCE IS DIFFERENT AND PUT SUCH ADDRESS IN OFFER

18a. PAYMENT WILL BE MADE BY — CODE: WEBVIEW

See Invoicing Instructions

18b. SUBMIT INVOICES TO ADDRESS SHOWN IN BLOCK 18a UNLESS BLOCK BELOW IS CHECKED ☐ SEE ADDENDUM

19. ITEM NO.	20. SCHEDULE OF SUPPLIES/SERVICES	21. QUANTITY	22. UNIT	23. UNIT PRICE	24. AMOUNT
	DUNS Number: 827431128+0000 This purchase order is Labor Hour (LH), Firm-Fixed Price (FFP) and Time-and-Material (T/M) with a base period of twelve months and two twelve(12)-month option periods. The purchase order is for Behavioral Threat Assessment, Consultation and Training for the USCIS Office of Human Capital and Training (HCT). Full Contract performance will begin when Notice to Proceed is issued by the Contracting Officer *(Use Reverse and/or Attach Additional Sheets as Necessary)*				

25. ACCOUNTING AND APPROPRIATION DATA
See schedule

26. TOTAL AWARD AMOUNT *(For Govt. Use Only)*
$71,250.00

☐ 27a. SOLICITATION INCORPORATES BY REFERENCE FAR 52.212-1, 52.212-4. FAR 52.212-3 AND 52.212-5 ARE ATTACHED. ADDENDA ☐ ARE ☐ ARE NOT ATTACHED.

☐ 27b. CONTRACT/PURCHASE ORDER INCORPORATES BY REFERENCE FAR 52.212-4. FAR 52.212-5 IS ATTACHED. ADDENDA ☐ ARE ☐ ARE NOT ATTACHED.

☒ 28. CONTRACTOR IS REQUIRED TO SIGN THIS DOCUMENT AND RETURN 1 COPIES TO ISSUING OFFICE. CONTRACTOR AGREES TO FURNISH AND DELIVER ALL ITEMS SET FORTH OR OTHERWISE IDENTIFIED ABOVE AND ON ANY ADDITIONAL SHEETS SUBJECT TO THE TERMS AND CONDITIONS SPECIFIED.

☒ 29. AWARD OF CONTRACT: 70SBUR19P00000128 OFFER DATED 09/30/2019. YOUR OFFER ON SOLICITATION (BLOCK 5), INCLUDING ANY ADDITIONS OR CHANGES WHICH ARE SET FORTH HEREIN, IS ACCEPTED AS TO ITEMS:

30a. SIGNATURE OF OFFEROR/CONTRACTOR	31a. UNITED STATES OF AMERICA *(SIGNATURE OF CONTRACTING OFFICER)*

30b. NAME AND TITLE OF SIGNER *(Type or print)*	30c. DATE SIGNED	31b. NAME OF CONTRACTING OFFICER *(Type or print)*	31c. DATE SIGNED
		Tiffany N. Vezina	

19. ITEM NO.	20. SCHEDULE OF SUPPLIES/SERVICES	21. QUANTITY	22. UNIT	23. UNIT PRICE	24. AMOUNT
	following satisfactory suitability determinations provided by the USCIS Office of Security and Integrity (OSI). Period of Performance: 09/30/2019 to 09/29/2022				
0001	Senior Consultation Services in accordance with Performance Work Statement (PWS Section 5.0) Labor Hour (LH) PoP 09/30/2019 - 09/29/2020 Accounting Info: SERVICE 000 EX 50-01-00-000 23-70-0300-00-00-00-00 GE-25-14-00 000000				
0002	Two-Day Training in accordance with Performance Work Statement (PWS Section 5.3.1) Firm-Fixed-Price (FFP) PoP 09/30/2019 - 09/29/2020 Accounting Info: SERVICE 000 EX 50-01-00-000 23-70-0300-00-00-00-00 GE-25-14-00 000000				
	Continued ...				

32a. QUANTITY IN COLUMN 21 HAS BEEN

☐ RECEIVED ☐ INSPECTED ☐ ACCEPTED, AND CONFORMS TO THE CONTRACT, EXCEPT AS NOTED: _____

32b. SIGNATURE OF AUTHORIZED GOVERNMENT REPRESENTATIVE	32c. DATE	32d. PRINTED NAME AND TITLE OF AUTHORIZED GOVERNMENT REPRESENTATIVE

32e. MAILING ADDRESS OF AUTHORIZED GOVERNMENT REPRESENTATIVE	32f. TELEPHONE NUMBER OF AUTHORIZED GOVERNMENT REPRESENTATIVE 32g. E-MAIL OF AUTHORIZED GOVERNMENT REPRESENTATIVE

33. SHIP NUMBER ☐ PARTIAL ☐ FINAL	34. VOUCHER NUMBER	35. AMOUNT VERIFIED CORRECT FOR	36. PAYMENT ☐ COMPLETE ☐ PARTIAL ☐ FINAL	37. CHECK NUMBER

38. S/R ACCOUNT NUMBER	39. S/R VOUCHER NUMBER	40. PAID BY

41a. I CERTIFY THIS ACCOUNT IS CORRECT AND PROPER FOR PAYMENT		42a. RECEIVED BY *(Print)*	
41b. SIGNATURE AND TITLE OF CERTIFYING OFFICER	41c. DATE	42b. RECEIVED AT *(Location)*	
		42c. DATE REC'D *(YY/MM/DD)*	42d. TOTAL CONTAINERS

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
0003	Other Direct Costs (Travel) in accordance with Performance Work Statement (PWS Section 7.0) ***NOT TO EXCEED $ 0.00*** Time-and-Material (T/M) PoP 09/30/2019 - 09/29/2020 Accounting Info: SERVICE 000 EX 50-01-00-000 23-70-0300-00-00-00-00 GE-25-14-00 000000 Funded: $ 0.00				
1001	Senior Consultation Services in accordance with Performance Work Statement (PWS Section 5.0) LH PoP 09/30/2020 - 09/29/2021 Amount: $ 0.00(Option Line Item) Anticipated Exercise Date:09/30/2020 Accounting Info: Funded: $0.00				
1002	Two-Day Training in accordance with Performance Work Statement (PWS Section 5.3.1) FFP PoP 09/30/2020 - 09/29/2021 Amount: $ 0.00(Option Line Item) Anticipated Exercise Date:09/30/2020 Accounting Info: Funded: $0.00				
1003	Other Direct Costs (Travel) in accordance with Performance Work Statement (PWS Section 7.0) ***NOT TO EXCEED $ 0.00*** T/M PoP 09/30/2020 - 09/29/2021 Amount: $ 0.00(Option Line Item) Anticipated Exercise Date:09/30/2020 Continued ...				

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	Accounting Info: Funded: $0.00				
2001	Senior Consultation Services in accordance with Performance Work Statement (PWS Section 5.0) LH PoP 09/30/2021 - 09/29/2022 Amount: $ 0.00(Option Line Item) Anticipated Exercise Date:09/30/2021 Accounting Info: Funded: $0.00				
2002	Two-Day Training in accordance with Performance Work Statement (PWS Section 5.3.1) FFP PoP 09/30/2021 - 09/29/2022 Amount: $ 0.00(Option Line Item) Anticipated Exercise Date:09/30/2021 Accounting Info: Funded: $0.00				
2003	Other Direct Costs (Travel) in accordance with Performance Work Statement (PWS Section 7.0) ***NOT TO EXCEED $ 0.00*** T/M PoP 09/30/2021 - 09/29/2022 Amount: $ 0.00(Option Line Item) Anticipated Exercise Date:09/30/2021 Accounting Info: Funded: $0.00 CONTRACT ADMINISTRATION: The contractor shall not accept any instruction that would result in any change to the supplies or services herein by any entity other than the issuing office's Contracting Officer (CO). The delegation for the Contracting Officers Technical Representative (COTR) will be assigned in accordance with HSAR Clause 3052.242-72, Continued ...				

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	Contracting Officers Technical Representative (COTR). The following is delegated to the Contract Specialist (CS). The CS is a procurement official who assists the CO in all aspects of the contracting functions. The CS will review and approve proper, accurate, and complete invoices for FFP contracts, and forward the approved invoices for payment processing. The CS will work with all involved to resolve any invoicing issues and insure the invoice documentation is accurate in the electronic record. The total amount of award: $ 0.00. The obligation for this award is shown in box 26.				

PART I – SF 1449

PART II – CONTRACT CLAUSES

Federal Acquisition Regulations (FAR) clauses incorporated by reference

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): FAR & HSAR CLAUSES: http://farsite.hill.af.mil/

(End of clause)

52.204-13 SYSTEM FOR AWARD MANAGEMNT MAINTENANCE (OCT 2018)

52.204-18 COMMERCIAL AND GOVERNMENT ENTITY CODE (JUL 2016)

52.204-19 INCORPORATION BY REFERENCE OF REPRESENTATIONS AND CERTIFICATIONS (DEC 2014)

52.212-4 CONTACT TERMS AND CONDITIONS-COMMERCIAL ITEM (OCT 2018)

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

52.212-5 CONTRACT TERMS AND CONDITIONS REQUIRED TO IMPLEMENT STATUTES OR EXECUTIVE ORDERS-COMMERCIAL ITEMS (AUG 2019)

(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) 52.203-19, Prohibition on Requiring Certain Internal Confidentiality Agreements or Statements (Jan 2017) (section 743 of Division E, Title VII, of the Consolidated and Further Continuing Appropriations Act, 2015 (Pub. L. 113-235) and its successor provisions in subsequent appropriations acts (and as extended in continuing resolutions)).

(2) 52.204-23, Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities (Jul 2018) (Section 1634 of Pub. L. 115-91).

(3) 52.204-25, Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment. (Aug 2019) (Section 889(a)(1)(A) of Pub. L. 115-232).

(4) 52.209-10, Prohibition on Contracting with Inverted Domestic Corporations (Nov 2015).

(5) 52.233-3, Protest After Award (Aug 1996) (31 U.S.C. 3553).

(6) 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:

_X_ (1) 52.203-6, Restrictions on Subcontractor Sales to the Government (Sept 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 (Oct 2015) (41 U.S.C. 3509)).
__ (3) 52.203-15, Whistleblower Protections under the American Recovery and Reinvestment Act of 2009 (June 2010) (Section 1553 of Pub. L. 111-5). (Applies to contracts funded by the American Recovery and Reinvestment Act of 2009.)
_X_ (4) 52.204-10, Reporting Executive Compensation and First-Tier Subcontract Awards (Oct 2018) (Pub. L. 109-282) (31 U.S.C. 6101 note).
__ (5) [Reserved].
__ (6) 52.204-14, Service Contract Reporting Requirements (Oct 2016) (Pub. L. 111-117, section 743 of Div. C).
__ (7) 52.204-15, Service Contract Reporting Requirements for Indefinite-Delivery Contracts (Oct 2016) (Pub. L. 111-117, section 743 of Div. C).
_X_ (8) 52.209-6, Protecting the Government's Interest When Subcontracting with Contractors Debarred, Suspended, or Proposed for Debarment. (Oct 2015) (31 U.S.C. 6101 note).
__ (9) 52.209-9, Updates of Publicly Available Information Regarding Responsibility Matters (Oct 2018) (41 U.S.C. 2313).
__ (10) [Reserved].
__ (11) (i) 52.219-3, Notice of HUBZone Set-Aside or Sole-Source Award (Nov 2011) (15 U.S.C.657a).
__ (ii) Alternate I (Nov 2011) of 52.219-3.
__ (12) (i) 52.219-4, Notice of Price Evaluation Preference for HUBZone Small Business Concerns (Oct 2014) (if the offeror elects to waive the preference, it shall so indicate in its offer) (15 U.S.C. 657a).
__ (ii) Alternate I (Jan 2011) of 52.219-4.
__ (13) [Reserved]
X (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 (June 2003) (15 U.S.C. 644).
__ (ii) Alternate I (Oct 1995) of 52.219-7.
__ (iii) Alternate II (Mar 2004) of 52.219-7.
_X_ (16) 52.219-8, Utilization of Small Business Concerns (Oct 2018) (15 U.S.C. 637(d)(2) and (3)).
__ (17) (i) 52.219-9, Small Business Subcontracting Plan (Aug 2018) (15 U.S.C. 637(d)(4))
__ (ii) Alternate I (Nov 2016) of 52.219-9.
__ (iii) Alternate II (Nov 2016) of 52.219-9.
__ (iv) Alternate III (Nov 2016) of 52.219-9.
__ (v) Alternate IV (Aug 2018) of 52.219-9
_X_ (18) 52.219-13, Notice of Set-Aside of Orders (Nov 2011) (15 U.S.C. 644(r)).
_X_ (19) 52.219-14, Limitations on Subcontracting (Jan 2017) (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) 52.219-27, Notice of Service-Disabled Veteran-Owned Small Business Set-Aside (Nov 2011) (15 U.S.C. 657f).
_X_ (22) 52.219-28, Post Award Small Business Program Rerepresentation (Jul 2013) (15 U.S.C. 632(a)(2)).
__ (23) 52.219-29, Notice of Set-Aside for, or Sole Source Award to, Economically Disadvantaged Women-Owned Small Business Concerns (Dec 2015) (15 U.S.C. 637(m)).

__ (24) 52.219-30, Notice of Set-Aside for, or Sole Source Award to, Women-Owned Small Business Concerns Eligible Under the Women-Owned Small Business Program (Dec 2015) (15 U.S.C. 637(m)).
_X_ (25) 52.222-3, Convict Labor (June 2003) (E.O.11755).
__ (26) 52.222-19, Child Labor-Cooperation with Authorities and Remedies (Jan 2018) (E.O.13126).
_X_ (27) 52.222-21, Prohibition of Segregated Facilities (Apr 2015).
__X (28) (i) 52.222-26, Equal Opportunity (Sept 2016) (E.O.11246).
__ (ii) Alternate I (Feb 1999) of 52.222-26.
__ (29) (i) 52.222-35, Equal Opportunity for Veterans (Oct 2015) (38 U.S.C. 4212).
__ (ii) Alternate I (July 2014) of 52.222-35.
__ (30) (i) 52.222-36, Equal Opportunity for Workers with Disabilities (Jul 2014) (29 U.S.C.793).
__ (ii) Alternate I (July 2014) of 52.222-36.
__ (31) 52.222-37, Employment Reports on Veterans (Feb 2016) (38 U.S.C. 4212).
_X_ (32) 52.222-40, Notification of Employee Rights Under the National Labor Relations Act (Dec 2010) (E.O. 13496).
_X_ (33) (i) 52.222-50, Combating Trafficking in Persons (Jan 2019) (22 U.S.C. chapter 78 and E.O. 13627).
__ (ii) Alternate I (Mar 2015) of 52.222-50 (22 U.S.C. chapter 78 and E.O. 13627).
_X_ (34) 52.222-54, Employment Eligibility Verification (Oct 2015). (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.)
__ (35) (i) 52.223-9, Estimate of Percentage of Recovered Material Content for EPA–Designated 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.)
__ (36) 52.223-11, Ozone-Depleting Substances and High Global Warming Potential Hydrofluorocarbons (Jun 2016) (E.O. 13693).
__ (37) 52.223-12, Maintenance, Service, Repair, or Disposal of Refrigeration Equipment and Air Conditioners (Jun2016) (E.O. 13693).
__ (38) (i) 52.223-13, Acquisition of EPEAT®-Registered Imaging Equipment (Jun 2014) (E.O.s 13423 and 13514).
__ (ii) Alternate I (Oct 2015) 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 (Oct 2015) (E.O.s 13423 and 13514).
__ (ii) Alternate I (Jun 2014) of 52.223-16.
_X_ (42) 52.223-18, Encouraging Contractor Policies to Ban Text Messaging While Driving (Aug 2011) (E.O. 13513).
__ (43) 52.223-20, Aerosols (Jun 2016) (E.O. 13693).
__ (44) 52.223-21, Foams (Jun 2016) (E.O. 13693).
_X_ (45) (i) 52.224-3 Privacy Training (Jan 2017) (5 U.S.C. 552 a).
_X_ (ii) Alternate I (Jan 2017) of 52.224-3.
__ (46) 52.225-1, Buy American-Supplies (May 2014) (41 U.S.C. chapter 83).
__ (47) (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.

__ (48) 52.225-5, Trade Agreements (Aug 2018) (19 U.S.C. 2501, et seq., 19 U.S.C. 3301 note).

_X_ (49) 52.225-13, Restrictions on Certain Foreign Purchases (June 2008) (E.O.'s, proclamations, and statutes administered by the Office of Foreign Assets Control of the Department of the Treasury).

__ (50) 52.225-26, Contractors Performing Private Security Functions Outside the United States (Oct 2016) (Section 862, as amended, of the National Defense Authorization Act for Fiscal Year 2008; 10 U.S.C. 2302 Note).

__ (51) 52.226-4, Notice of Disaster or Emergency Area Set-Aside (Nov 2007) (42 U.S.C. 5150).

__ (52) 52.226-5, Restrictions on Subcontracting Outside Disaster or Emergency Area (Nov 2007) (42 U.S.C. 5150).

__ (53) 52.232-29, Terms for Financing of Purchases of Commercial Items (Feb 2002) (41 U.S.C.4505, 10 U.S.C.2307(f)).

__ (54) 52.232-30, Installment Payments for Commercial Items (Jan 2017) (41 U.S.C.4505, 10 U.S.C.2307(f)).

_X_ (55) 52.232-33, Payment by Electronic Funds Transfer-System for Award Management (Oct 2018) (31 U.S.C. 3332).

__ (56) 52.232-34, Payment by Electronic Funds Transfer-Other than System for Award Management (Jul 2013) (31 U.S.C.3332).

__ (57) 52.232-36, Payment by Third Party (May 2014) (31 U.S.C.3332).

__ (58) 52.239-1, Privacy or Security Safeguards (Aug 1996) (5 U.S.C. 552a).

__ (59) 52.242-5, Payments to Small Business Subcontractors (Jan 2017) (15 U.S.C. 637(d)(13)).

__ (60) (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.

__ (iii) Alternate II (Feb 2006) 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) 52.222-17, Nondisplacement of Qualified Workers (May 2014)(E.O. 13495).

__ (2) 52.222-41, Service Contract Labor Standards (Aug 2018) (41 U.S.C. chapter 67).

__ (3) 52.222-42, Statement of Equivalent Rates for Federal Hires (May 2014) (29 U.S.C. 206 and 41 U.S.C. chapter 67).

__ (4) 52.222-43, Fair Labor Standards Act and Service Contract Labor Standards-Price Adjustment (Multiple Year and Option Contracts) (Aug 2018) (29 U.S.C. 206 and 41 U.S.C. chapter 67).

__ (5) 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).

__ (6) 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).

__ (7) 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).

__ (8) 52.222-55, Minimum Wages Under Executive Order 13658 (Dec 2015).
__ (9) 52.222-62, Paid Sick Leave Under Executive Order 13706 (Jan 2017) (E.O. 13706).
__ (10) 52.226-6, Promoting Excess Food Donation to Nonprofit Organizations (May 2014) (42 U.S.C. 1792).

(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 this paragraph (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 (Oct 2015) (41 U.S.C. 3509).
(ii) 52.203-19, Prohibition on Requiring Certain Internal Confidentiality Agreements or Statements (Jan 2017) (section 743 of Division E, Title VII, of the Consolidated and Further Continuing Appropriations Act, 2015 (Pub. L. 113-235) and its successor provisions in subsequent appropriations acts (and as extended in continuing resolutions)).
(iii) 52.204-23, Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities (Jul 2018) (Section 1634 of Pub. L. 115-91).
(iv) 52.204-25, Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment. (Aug 2019) (Section 889(a)(1)(A) of Pub. L. 115-232).
(v) 52.219-8, Utilization of Small Business Concerns (Oct 2018) (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 $700,000 ($1.5 million for construction of any public facility), the subcontractor must include 52.219-8 in lower tier subcontracts that offer subcontracting opportunities.
(vi) 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.
(vii) 52.222-21, Prohibition of Segregated Facilities (Apr 2015).
(viii) 52.222-26, Equal Opportunity (Sept 2015) (E.O.11246).
(ix) 52.222-35, Equal Opportunity for Veterans (Oct 2015) (38 U.S.C.4212).
(x) 52.222-36, Equal Opportunity for Workers with Disabilities (Jul 2014) (29 U.S.C.793).
(xi) 52.222-37, Employment Reports on Veterans (Feb 2016) (38 U.S.C.4212)

(xii) 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.
(xiii) 52.222-41, Service Contract Labor Standards (Aug 2018) (41 U.S.C. chapter 67).
(xiv) (A) 52.222-50, Combating Trafficking in Persons (Jan 2019) (22 U.S.C. chapter 78 and E.O 13627).
(B) Alternate I (Mar 2015) of 52.222-50(22 U.S.C. chapter 78 and E.O 13627).
(xv) 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).
(xvi) 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).
(xvii) 52.222-54, Employment Eligibility Verification (Oct 2015) (E.O. 12989).
(xviii) 52.222-55, Minimum Wages Under Executive Order 13658 (Dec 2015).
(xix) 52.222-62, Paid Sick Leave Under Executive Order 13706 (Jan 2017) (E.O. 13706).
(xx) (A) 52.224-3, Privacy Training (Jan 2017) (5 U.S.C. 552a).
(B) Alternate I (Jan 2017) of 52.224-3.
(xxi) 52.225-26, Contractors Performing Private Security Functions Outside the United States (Oct 2016) (Section 862, as amended, of the National Defense Authorization Act for Fiscal Year 2008; 10 U.S.C. 2302 Note).
(xxii) 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.
(xxiii) 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)

Federal Acquisition Regulations (FAR) clauses incorporated in full text

52.217-8 OPTION TO EXTEND SERVICES (NOV 1999)

The Government may require continued performance of any services within the limits and at the rates specified in the contract. These rates may be adjusted only as a result of revisions to prevailing labor rates provided by the Secretary of Labor. The option provision may be exercised more than once, but the total extension of performance hereunder shall not exceed 6 months. The Contracting Officer may exercise the option by written notice to the Contractor within 60 Days.

(End of clause)

52.217-9 OPTION TO EXTEND THE TERM OF THE CONTRACT (MAR 2000)

(a) The Government may extend the term of this contract by written notice to the Contractor within 30 Days; provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least 60 days before the contract expires. The preliminary notice does not commit the Government to an extension.

(b) If the Government exercises this option, the extended contract shall be considered to include this option clause.

(c) The total duration of this contract, including the exercise of any options under this clause, shall not exceed 36 Months.

(End of clause)

Homeland Security Acquisition Regulation (HSAR) clauses incorporated by reference

3052.205-70 ADVERTISING, PUBLICIZING AWARDS, AND RELEASES (SEPT 2012)

3052.242-72 CONTRACTING OFFICER'S TECHNICAL REPRESENTATIVE (DEC 2003)

Homeland Security Acquisition Regulation (HSAR) clauses incorporated in full text

3052.204-71 CONTRACTOR EMPLOYEE ACCESS (SEP 2012)

(a) Sensitive Information, as used in this clause, means any information, which if lost, misused, disclosed, or, without authorization is accessed, or modified, could adversely affect the national or homeland security interest, the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense, homeland security or foreign policy. This definition includes the following categories of information:

(1) Protected Critical Infrastructure Information (PCII) as set out in the Critical Infrastructure Information Act of 2002 (Title II, Subtitle B, of the Homeland Security Act, Public Law 107-296, 196 Stat. 2135), as amended, the implementing regulations thereto (Title 6, Code of Federal Regulations, Part 29) as amended, the applicable PCII Procedures Manual, as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the PCII Program Manager or his/her designee);

(2) Sensitive Security Information (SSI), as defined in Title 49, Code of Federal Regulations, Part 1520, as amended, "Policies and Procedures of Safeguarding and Control of SSI," as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the Assistant Secretary for the Transportation Security Administration or his/her designee);

(3) Information designated as "For Official Use Only," which is unclassified information of a sensitive nature and the unauthorized disclosure of which could adversely impact a person's privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national or homeland security interest; and

(4) Any information that is designated "sensitive" or subject to other controls, safeguards or protections in accordance with subsequently adopted homeland security information handling procedures.

(b) "Information Technology Resources" include, but are not limited to, computer equipment, networking equipment, telecommunications equipment, cabling, network drives, computer drives, network software, computer software, software programs, intranet sites, and internet sites.

(c) Contractor employees working on this contract must complete such forms as may be necessary for security or other reasons, including the conduct of background investigations to determine suitability. Completed forms shall be submitted as directed by the Contracting Officer. Upon the Contracting Officer's request, the Contractor's employees shall be fingerprinted, or subject to other investigations as required. All Contractor employees requiring recurring access to Government facilities or access to sensitive information or IT resources are required

to have a favorably adjudicated background investigation prior to commencing work on this contract unless this requirement is waived under Departmental procedures.
(d) The Contracting Officer may require the Contractor to prohibit individuals from working on the contract if the Government deems their initial or continued employment contrary to the public interest for any reason, including, but not limited to, carelessness, insubordination, incompetence, or security concerns.
(e) Work under this contract may involve access to sensitive information. Therefore, the Contractor shall not disclose, orally or in writing, any sensitive information to any person unless authorized in writing by the Contracting Officer. For those Contractor employees authorized access to sensitive information, the Contractor shall ensure that these persons receive training concerning the protection and disclosure of sensitive information both during and after contract performance.
(f) The Contractor shall include the substance of this clause in all subcontracts at any tier where the subcontractor may have access to Government facilities, sensitive information, or resources.

(End of Clause)

Alternate I

When the contract will require contractor employees to have access to Information Technology (IT) resources, add the following paragraphs:
(g) Before receiving access to IT resources under this contract the individual must receive a security briefing, which the Contracting Officer's Technical Representative (COTR) will arrange, and complete any nondisclosure agreement furnished by DHS.
(h) The Contractor shall have access only to those areas of DHS information technology resources explicitly stated in this contract or approved by the COTR in writing as necessary for performance of the work under this contract. Any attempts by Contractor personnel to gain access to any information technology resources not expressly authorized by the statement of work, other terms and conditions in this contract, or as approved in writing by the COTR, is strictly prohibited. In the event of violation of this provision, DHS will take appropriate actions with regard to the contract and the individual(s) involved.
(i) Contractor access to DHS networks from a remote location is a temporary privilege for mutual convenience while the Contractor performs business for the DHS Component. It is not a right, a guarantee of access, a condition of the contract, or Government Furnished Equipment (GFE).
(j) Contractor access will be terminated for unauthorized use. The Contractor agrees to hold and save DHS harmless from any unauthorized use and agrees not to request additional time or money under the contract for any delays resulting from unauthorized use or access.
(k) Non-U.S. citizens shall not be authorized to access or assist in the development, operation, management or maintenance of Department IT systems under the contract, unless a waiver has been granted by the Head of the Component or designee, with the concurrence of both the Department's Chief Security Officer (CSO) and the Chief Information Officer (CIO) or their designees. Within DHS Headquarters, the waiver may be granted only with the approval of both the CSO and the CIO or their designees. In order for a waiver to be granted:
(1) There must be a compelling reason for using this individual as opposed to a U. S. citizen; and
(2) The waiver must be in the best interest of the Government.

(l) Contractors shall identify in their proposals the names and citizenship of all non-U.S. citizens proposed to work under the contract. Any additions or deletions of non-U.S. citizens after contract award shall also be reported to the Contracting Officer.

(End of Clause)

3052.209-70 PROHIBITION ON CONTRACTS WITH CORPORATE EXPATRIATES (JUN 2006)

(a) Prohibitions.

Section 835 of the Homeland Security Act, 6 U.S.C. 395, prohibits the Department of Homeland Security from entering into any contract with a foreign incorporated entity which is treated as an inverted domestic corporation as defined in this clause, or with any subsidiary of such an entity. The Secretary shall waive the prohibition with respect to any specific contract if the Secretary determines that the waiver is required in the interest of national security.

(b) Definitions. As used in this clause:

Expanded Affiliated Group means an affiliated group as defined in section 1504(a) of the Internal Revenue Code of 1986 (without regard to section 1504(b) of such Code), except that section 1504 of such Code shall be applied by substituting `more than 50 percent' for `at least 80 percent' each place it appears.

Foreign Incorporated Entity means any entity which is, or but for subsection (b) of section 835 of the Homeland Security Act, 6 U.S.C. 395, would be, treated as a foreign corporation for purposes of the Internal Revenue Code of 1986.

Inverted Domestic Corporation. A foreign incorporated entity shall be treated as an inverted domestic corporation if, pursuant to a plan (or a series of related transactions)—

(1) The entity completes the direct or indirect acquisition of substantially all of the properties held directly or indirectly by a domestic corporation or substantially all of the properties constituting a trade or business of a domestic partnership;

(2) After the acquisition at least 80 percent of the stock (by vote or value) of the entity is held—

(i) In the case of an acquisition with respect to a domestic corporation, by former shareholders of the domestic corporation by reason of holding stock in the domestic corporation; or

(ii) In the case of an acquisition with respect to a domestic partnership, by former partners of the domestic partnership by reason of holding a capital or profits interest in the domestic partnership; and

(3) The expanded affiliated group which after the acquisition includes the entity does not have substantial business activities in the foreign country in which or under the law of which the entity is created or organized when compared to the total business activities of such expanded affiliated group.

Person, domestic, and foreign have the meanings given such terms by paragraphs (1), (4), and (5) of section 7701(a) of the Internal Revenue Code of 1986, respectively.

(c) Special rules. The following definitions and special rules shall apply when determining whether a foreign incorporated entity should be treated as an inverted domestic corporation.

(1) Certain stock disregarded. For the purpose of treating a foreign incorporated entity as an inverted domestic corporation these shall not be taken into account in determining ownership:

(i) Stock held by members of the expanded affiliated group which includes the foreign incorporated entity; or

(ii) Stock of such entity which is sold in a public offering related to an acquisition described in section 835(b)(1) of the Homeland Security Act, 6 U.S.C. 395(b)(1).

(2) Plan deemed in certain cases. If a foreign incorporated entity acquires directly or indirectly substantially all of the properties of a domestic corporation or partnership during the 4-year period beginning on the date which is 2

years before the ownership requirements of subsection (b)(2) are met, such actions shall be treated as pursuant to a plan.
(3) Certain transfers disregarded. The transfer of properties or liabilities (including by contribution or distribution) shall be disregarded if such transfers are part of a plan a principal purpose of which is to avoid the purposes of this section.

(d) Special rule for related partnerships. For purposes of applying section 835(b) of the Homeland Security Act, 6 U.S.C. 395(b) to the acquisition of a domestic partnership, except as provided in regulations, all domestic partnerships which are under common control (within the meaning of section 482 of the Internal Revenue Code of 1986) shall be treated as a partnership.

(e) Treatment of Certain Rights.
(1) Certain rights shall be treated as stocks to the extent necessary to reflect the present value of all equitable interests incident to the transaction, as follows:
(i) warrants;
(ii) options;
(iii) contracts to acquire stock;
(iv) convertible debt instruments; and
(v) others similar interests.
(2) Rights labeled as stocks shall not be treated as stocks whenever it is deemed appropriate to do so to reflect the present value of the transaction or to disregard transactions whose recognition would defeat the purpose of Section 835.
(f) Disclosure. The offeror under this solicitation represents that [Check one]:

X it is not a foreign incorporated entity that should be treated as an inverted domestic corporation pursuant to the criteria of (HSAR) 48 CFR 3009.108-7001 through 3009.108-7003;
__ it is a foreign incorporated entity that should be treated as an inverted domestic corporation pursuant to the criteria of (HSAR) 48 CFR 3009.108-7001 through 3009.108-7003, but it has submitted a request for waiver pursuant to 3009.108-7004, which has not been denied; or
__ it is a foreign incorporated entity that should be treated as an inverted domestic corporation pursuant to the criteria of (HSAR) 48 CFR 3009.108-7001 through 3009.108-7003, but it plans to submit a request for waiver pursuant to 3009.108-7004.

(g) A copy of the approved waiver, if a waiver has already been granted, or the waiver request, if a waiver has been applied for, shall be attached to the bid or proposal.

(End of clause)

United States Citizenship and Immigration Services (USCIS) Local Clauses

INVOICING REQUIREMENTS:

In accordance with FAR Part 52.212-4(g) Contract Terms and Conditions -- Commercial Items (OCT 2018)

(a) The Contractor shall submit an original invoice and three copies (or electronic invoice, if authorized) to the address designated in the contract to receive invoices. An invoice must include:
(i) Name and address of the Contractor;
(ii) Invoice date and number;

(iii) Contract number, line item number and, if applicable, the order number;
(iv) Description, quantity, unit of measure, unit price and extended price of the items delivered;
(v) Shipping number and date of shipment, including the bill of lading number and weight of shipment if shipped on Government bill of lading;
(vi) Terms of any discount for prompt payment offered;
(vii) Name and address of official to whom payment is to be sent;
(viii) Name, title, and phone number of person to notify in event of defective invoice; and
(ix) Taxpayer Identification Number (TIN). The Contractor shall include its TIN on the invoice only if required elsewhere in this contract.
(x) Electronic funds transfer (EFT) banking information.

(b) USCIS' preferred method for invoice submission is electronically. Invoices shall be submitted in Adobe pdf format with each pdf file containing only one invoice. The pdf files shall be submitted electronically using the "To" line in the e-mail address to USCISInvoice.Consolidation@ice.dhs.gov with each email conforming to a size limit of 500 KB.

If a paper invoice is submitted, mail the invoice to:

USCIS Invoice Consolidation

PO Box 1000

Williston, VT 05495

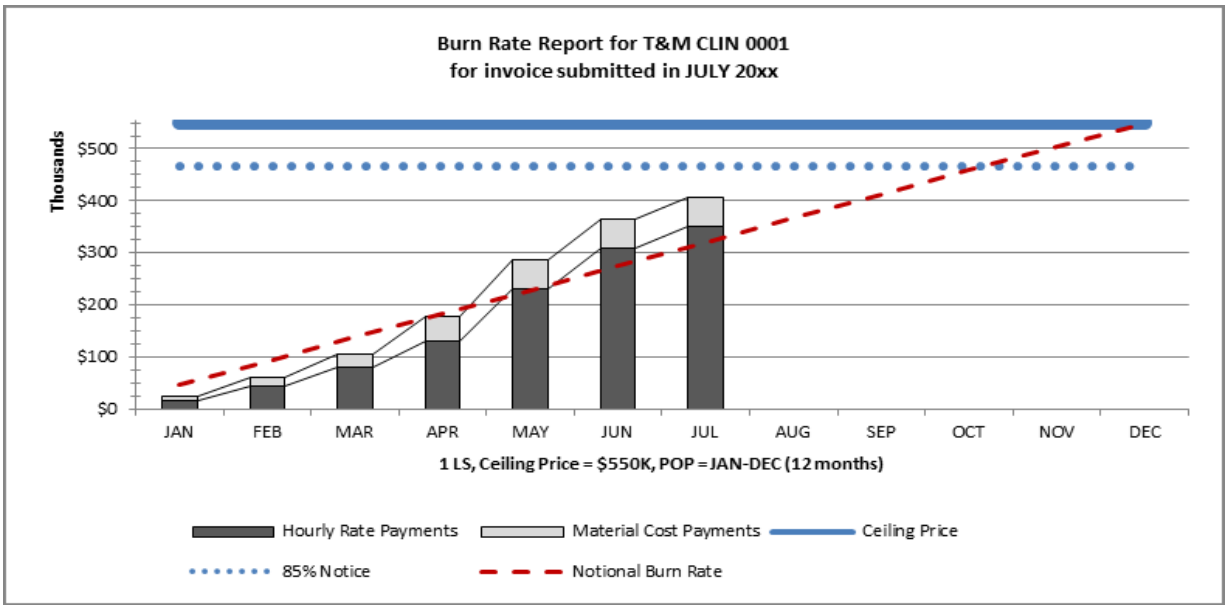
DIRECT PAYMENT INQUIRIES TO ICE FINANCIAL OPERATIONS, (877) 491-6521

(c) Invoices not meeting these requirements will be rejected and not paid until a corrected invoice meeting the requirements is received.

(d) BURN RATE CHART AND TABLE DELIVERABLES

1) The Contractor shall submit a chart and table, in the Contractor's format as approved by the contracting officer, showing its projected and actual burn rates for each time-and-materials (T&M) or labor-hour (LH) CLIN as supporting documentation for each invoice or voucher it submits to the Government for payment. This requirement is a material term of this contract or order, and is a condition of a proper invoice or voucher.

2) The chart shall display the current period of performance, the ceiling price, and the cumulative amounts for hourly rate charges and materials charges for the instant and all previous invoices or vouchers submitted during the current period of performance. A notional sample is provided below for the convenience of the Contractor—



3) The table shall include all the data used to develop the chart, and may include additional data that might be helpful in the Government's understanding of the Contractor's progress and experience under the contract or order.

4) Nothing in this section relieves the Contractor of its responsibility to give timely and proper notice to the contracting officer of the possibility of exceeding the ceiling price. The chart and table called for by this section shall not serve as that notice.

(e) Invoices for hours incurred under LH or T&M CLINs shall also include a breakdown by contractor employee and period to ensure invoices can be approved in a timely fashion. Delayed costs, including travel receipts and subcontract labor, shall be clearly identified as to the period in which the costs were incurred.

(End of clause)

Posting of Order in FOIA Reading Room

(a) The Government intends to post the order resulting from this solicitation to a public FOIA reading room.
(b) Within 30 days of award, the contractor shall submit a redacted copy of the executed or order (including all attachments) suitable for public posting under the provisions of the Freedom of Information Act (FOIA). The contractor shall submit the documents to the USCIS FOIA Office by email at foiaerr.nrc@uscis.dhs.gov with a courtesy copy to the contracting officer.
(c) The USCIS FOIA Office will notify the contractor of any disagreements with the contractor's redactions before public posting of the contract or order in a public FOIA reading room.

(End of Clause)

SECURITY CLAUSE 5

GENERAL

U.S. Citizenship and Immigration Services (USCIS) has determined that performance of this contract requires that the Contractor, subcontractor(s), vendor(s), etc. (herein known as Contractor), requires access to sensitive but unclassified information, and that the Contractor will adhere to the following.

SUITABILITY DETERMINATION

USCIS shall have and exercise full control over granting, denying, withholding or terminating access of unescorted Contractor employees to government facilities and/or access of Contractor employees to sensitive but unclassified information based upon the results of a background investigation.

USCIS may, as it deems appropriate, authorize and make a favorable entry on duty (EOD) decision based on preliminary security checks. The favorable EOD decision would allow the employees to commence work temporarily prior to the completion of the full investigation. The granting of a favorable EOD decision shall not be considered as assurance that a full employment suitability authorization will follow as a result thereof. The granting of a favorable EOD decision or a full employment suitability determination shall in no way prevent, preclude, or bar the withdrawal or termination of any such access by USCIS, at any time during the term of the contract. No Contractor employee shall be allowed unescorted access to a Government facility without a favorable EOD decision or suitability determination by the Office of Security & Integrity Personnel Security Division (OSI PSD).

BACKGROUND INVESTIGATIONS

Contractor employees (to include applicants, temporaries, part-time and replacement employees) under the contract, needing access to sensitive but unclassified information shall undergo a position sensitivity analysis based on the duties each individual will perform on the contract as outlined in the DHS Form 11000-25, Contractor Fitness/Security Screening Request Form and the USCIS Continuation Page to the DHS Form 11000-25. The results of the position sensitivity analysis shall identify the appropriate background investigation to be conducted. All background investigations will be processed through OSI PSD.

To the extent the DHS Form 11000-25 and the USCIS Continuation Page to the DHS Form 11000- 25 reveals that the Contractor will not require access to sensitive but unclassified information or access to USCIS IT systems, OSI PSD may determine that preliminary security screening and or a complete background investigation is not required for performance on this contract.

Completed packages must be submitted to OSI PSD for prospective Contractor employees no less than 30 days before the starting date of the contract or 30 days prior to EOD of any employees, whether a replacement, addition, subcontractor employee, or vendor. The Contractor shall follow guidelines for package submission as set forth by OSI PSD. A complete package will include the following forms, in conjunction with security questionnaire submission of the SF-85P, "Security Questionnaire for Public Trust Positions" via e-QIP:

1. DHS Form 11000-6, "Conditional Access to Sensitive But Unclassified Information Non-Disclosure Agreement"

2. FD Form 258, "Fingerprint Card" **(2 copies)**

3. Form DHS 11000-9, "Disclosure and Authorization Pertaining to Consumer Reports Pursuant to the Fair Credit Reporting Act"

4. DHS Form 11000-25 "Contractor Fitness/Security Screening Request Form"

5. USCIS Continuation Page to DHS Form 11000-25

6. OF 306, Declaration for Federal Employment (approved use for FederalContract Employment)

7. Foreign National Relatives or Associates Statement

EMPLOYMENT ELIGIBILITY

Be advised that unless an applicant requiring access to sensitive but unclassified information has resided in the U.S. for three of the past five years, OSI PSD may not be able to complete a satisfactory background investigation. In such cases, USCIS retains the right to deem an applicant as ineligible due to insufficient background information.

Only U.S. citizens are eligible for employment on contracts requiring access to Department of Homeland Security (DHS) Information Technology (IT) systems or involvement in the development, operation, management, or maintenance of DHS IT systems, unless a waiver has been granted by the Director of USCIS, or designee, with the concurrence of both the DHS Chief Security Officer and the Chief Information Officer or their designees. In instances where non-IT requirements contained in the contract can be met by using Legal Permanent Residents, those requirements shall be clearly described.

The Contractor must agree that each employee working on this contract will have a Social Security Card issued by the Social Security Administration.

CONTINUED ELIGIBILITY

If a prospective employee is found to be ineligible for access to USCIS facilities or information, the Contracting Officer's Representative (COR) will advise the Contractor that the employee shall not continue to work or to be assigned to work under the contract.

In accordance with USCIS policy, contractors are required to undergo a periodic reinvestigation every five years. Security documents will be submitted to OSI PSD within ten business days following notification of a contractor's reinvestigation requirement.

In support of the overall USCIS mission, Contractor employees are required to complete one-time or annual DHS/USCIS mandatory trainings. The Contractor shall certify annually, but no later than December 31st each year, or prior to any accelerated deadlines designated by USCIS, that required trainings have been completed. The certification of the completion of the trainings by all contractors shall be provided to both the COR and Contracting Officer.

- **USCIS Security Awareness Training** (required within 30 days of entry on dutyfor new contractors, and annually thereafter)
- **USCIS Integrity Training** (Annually)
- **DHS Insider Threat Training** (Annually)
- **DHS Continuity of Operations Awareness Training** (one-time training for contractors identified as providing an essential service)
- **Unauthorized Disclosure Training** (one time training for contractors who require access to USCIS information regardless if performance occurs within USCIS facilities or at a company owned and operated facility)
- **USCIS Fire Prevention and Safety Training** (one-time training for contractors working within USCIS facilities; contractor companies may substitute their owntraining)

- **Computer Security Awareness Training** (if contractor requires access to USCIS IT systems, training must be completed within 60 days of entry on duty for new contractors, and annually thereafter)

USCIS reserves the right and prerogative to deny and/or restrict the facility and information access of any Contractor employee whose actions are in conflict with the standards of conduct or whom USCIS determines to present a risk of compromising sensitive but unclassified information and/or classified information.

Contract employees will report any adverse information concerning their personal conduct to OSI PSD. The report shall include the contractor's name along with the adverse information being reported. Required reportable adverse information includes, but is not limited to, criminal charges and or arrests, negative change in financial circumstances, and any additional information that requires admission on the SF-85P security questionnaire.

In accordance with Homeland Security Presidential Directive-12 (HSPD-12) http://www.dhs.gov/homeland-security-presidential-directive-12 contractor employees who require access to United States Citizenship and Immigration Services (USCIS) facilities and/or utilize USCIS Information Technology (IT) systems, must be issued and maintain a Personal Identity Verification (PIV) card throughout the period of performance on their contract. Government-owned contractor- operated facilities are considered USCIS facilities.

After the Office of Security & Integrity, Personnel Security Division has notified the Contracting Officer's Representative that a favorable entry on duty (EOD) determination has been rendered, contractor employees will need to obtain a PIV card.

For new EODs, contractor employees have [*10 business days unless a different number is inserted*] from their EOD date to comply with HSPD-12. For existing EODs, contractor employees have [*10 business days unless a different number of days is inserted*] from the date this clause is incorporated into the contract to comply with HSPD-12.

Contractor employees who do not have a PIV card must schedule an appointment to have one issued. To schedule an appointment:
http://ecn.uscis.dhs.gov/team/mgmt/Offices/osi/FSD/HSPD12/PIV/default.aspx

Contractors who are unable to access the hyperlink above shall contact the Contracting Officer's Representative (COR) for assistance.

Contractor employees who do not have a PIV card will need to be escorted at all times by a government employee while at a USCIS facility and will not be allowed access to USCIS IT systems.

A contractor employee required to have a PIV card shall:

- Properly display the PIV card above the waist and below the neck with the photo facing outso that it is visible at all times while in a USCIS facility
- Keep their PIV card current
- Properly store the PIV card while not in use to prevent against loss or theft

http://ecn.uscis.dhs.gov/team/mgmt/Offices/osi/FSD/HSPD12/SIR/default.aspx

OSI PSD must be notified of all terminations/ resignations within five days of occurrence. The Contractor will return any expired USCIS issued identification cards and HSPD-12 card, or those of terminated employees to

the COR. If an identification card or HSPD-12 card is not available to be returned, a report must be submitted to the COR, referencing the card number, name of individual to whom issued, the last known location and disposition of the card.

SECURITY MANAGEMENT

The Contractor shall appoint a senior official to act as the Corporate Security Officer. The individual will interface with OSI through the COR on all security matters, to include physical, personnel, and protection of all Government information and data accessed by the Contractor.

The COR and OSI shall have the right to inspect the procedures, methods, and facilities utilized by the Contractor in complying with the security requirements under this contract. Should the COR determine that the Contractor is not complying with the security requirements of this contract the Contractor will be informed in writing by the Contracting Officer of the proper action to be taken in order to effect compliance with such requirements.

The Contractor shall be responsible for all damage or injuries resulting from the acts or omissions of their employees and/or any subcontractor(s) and their employees to include financial responsibility.

(End of Clause)

Safeguarding of Sensitive Information (MAR 2015)

(a) Applicability. This clause applies to the Contractor, its subcontractors, and Contractor employees (hereafter referred to collectively as "Contractor"). The Contractor shall insert the substance of this clause in all subcontracts.

(b) Definitions. As used in this clause—

"Personally Identifiable Information (PII)" means information that can be used to distinguish or trace an individual's identity, such as name, social security number, or biometric records, either alone, or when combined with other personal or identifying information that is linked or linkable to a specific individual, such as date and place of birth, or mother's maiden name. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. In performing this assessment, it is important for an agency to recognize that non-personally identifiable information can become personally identifiable information whenever additional information is made publicly available—in any medium and from any source—that, combined with other available information, could be used to identify an individual.

PII is a subset of sensitive information. Examples of PII include, but are not limited to: name, date of birth, mailing address, telephone number, Social Security number (SSN), email address, zip code, account numbers, certificate/license numbers, vehicle identifiers including license plates, uniform resource locators (URLs), static Internet protocol addresses, biometric identifiers such as fingerprint, voiceprint, iris scan, photographic facial images, or any other unique identifying number or characteristic, and any information where it is reasonably foreseeable that the information will be linked with other information to identify the individual.

"Sensitive Information" is defined in HSAR clause 3052.204-71, Contractor Employee Access, as any information, which if lost, misused, disclosed, or, without authorization is accessed, or modified, could adversely affect the national or homeland security interest, the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of Title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or

an Act of Congress to be kept secret in the interest of national defense, homeland security or foreign policy. This definition includes the following categories of information:

(1) Protected Critical Infrastructure Information (PCII) as set out in the Critical Infrastructure Information Act of 2002 (Title II, Subtitle B, of the Homeland Security Act, Public Law 107-296, 196 Stat. 2135), as amended, the implementing regulations thereto (Title 6, Code of Federal Regulations, Part 29) as amended, the applicable PCII Procedures Manual, as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the PCII Program Manager or his/her designee);

(2) Sensitive Security Information (SSI), as defined in Title 49, Code of Federal Regulations, Part 1520, as amended, "Policies and Procedures of Safeguarding and Control of SSI," as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the Assistant Secretary for the Transportation Security Administration or his/her designee);

(3) Information designated as "For Official Use Only," which is unclassified information of a sensitive nature and the unauthorized disclosure of which could adversely impact a person's privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national or homeland security interest; and

(4) Any information that is designated "sensitive" or subject to other controls, safeguards or protections in accordance with subsequently adopted homeland security information handling procedures.

"Sensitive Information Incident" is an incident that includes the known, potential, or suspected exposure, loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or unauthorized access or attempted access of any Government system, Contractor system, or sensitive information.

"Sensitive Personally Identifiable Information (SPII)" is a subset of PII, which if lost, compromised or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Some forms of PII are sensitive as stand-alone elements. Examples of such PII include: Social Security numbers (SSN), driver's license or state identification number, Alien Registration Numbers (A-number), financial account number, and biometric identifiers such as fingerprint, voiceprint, or iris scan. Additional examples include any groupings of information that contain an individual's name or other unique identifier plus one or more of the following elements:

(1) Truncated SSN (such as last 4 digits)
(2) Date of birth (month, day, and year)
(3) Citizenship or immigration status
(4) Ethnic or religious affiliation
(5) Sexual orientation
(6) Criminal History
(7) Medical Information
(8) System authentication information such as mother's maiden name, account passwords or personal identification numbers (PIN)

Other PII may be "sensitive" depending on its context, such as a list of employees and their performance ratings or an unlisted home address or phone number. In contrast, a business card or public telephone directory of agency employees contains PII but is not sensitive.

(c) Authorities. The Contractor shall follow all current versions of Government policies and guidance accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors, or available upon request from the Contracting Officer, Including but not limited to:

(1) DHS Management Directive 11042.1 Safeguarding Sensitive But Unclassified (for Official Use Only) Information
(2) DHS Sensitive Systems Policy Directive 4300A
(3) DHS 4300A Sensitive Systems Handbook and Attachments
(4) DHS Security Authorization Process Guide
(5) DHS Handbook for Safeguarding Sensitive Personally Identifiable Information
(6) DHS Instruction Handbook 121-01-007 Department of Homeland Security Personnel Suitability and Security Program
(7) DHS Information Security Performance Plan (current fiscal year)
(8) DHS Privacy Incident Handling Guidance
(9) Federal Information Processing Standard (FIPS) 140-2 Security Requirements for Cryptographic Modules accessible at http://csrc.nist.gov/groups/STM/cmvp/standards.html
(10) National Institute of Standards and Technology (NIST) Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations accessible at http://csrc.nist.gov/publications/PubsSPs.html
(11) NIST Special Publication 800-88 Guidelines for Media Sanitization accessible at http://csrc.nist.gov/publications/PubsSPs.html

(d) Handling of Sensitive Information. Contractor compliance with this clause, as well as the policies and procedures described below, is required.

(1) Department of Homeland Security (DHS) policies and procedures on Contractor personnel security requirements are set forth in various Management Directives (MDs), Directives, and Instructions. MD 11042.1, Safeguarding Sensitive But Unclassified (For Official Use Only) Information describes how Contractors must handle sensitive but unclassified information. DHS uses the term "FOR OFFICIAL USE ONLY" to identify sensitive but unclassified information that is not otherwise categorized by statute or regulation. Examples of sensitive information that are categorized by statute or regulation are PCII, SSI, etc. The DHS Sensitive Systems Policy Directive 4300A and the DHS 4300A Sensitive Systems Handbook provide the policies and procedures on security for Information Technology (IT) resources. The DHS Handbook for Safeguarding Sensitive Personally Identifiable Information provides guidelines to help safeguard SPII in both paper and electronic form. DHS Instruction Handbook 121-01-007 Department of Homeland Security Personnel Suitability and Security Program establishes procedures, program responsibilities, minimum standards, and reporting protocols for the DHS Personnel Suitability and Security Program.

(2) The Contractor shall not use or redistribute any sensitive information processed, stored, and/or transmitted by the Contractor except as specified in the contract.

(3) All Contractor employees with access to sensitive information shall execute DHS Form 11000-6, Department of Homeland Security Non-Disclosure Agreement (NDA), as a condition of access to such information. The Contractor shall maintain signed copies of the NDA for all employees as a record of compliance. The Contractor shall provide copies of the signed NDA to the Contracting Officer's Representative (COR) no later than two (2) days after execution of the form.

(4) The Contractor's invoicing, billing, and other recordkeeping systems maintained to support financial or other administrative functions shall not maintain SPII. It is acceptable to maintain in these systems the names, titles and contact information for the COR or other Government personnel associated with the administration of the contract, as needed.

(e) Authority to Operate. The Contractor shall not input, store, process, output, and/or transmit sensitive information within a Contractor IT system without an Authority to Operate (ATO) signed by the Headquarters or Component CIO, or designee, in consultation with the Headquarters or Component Privacy Officer. Unless otherwise specified in the ATO letter, the ATO is valid for

three (3) years. The Contractor shall adhere to current Government policies, procedures, and guidance for the Security Authorization (SA) process as defined below.

(1) Complete the Security Authorization process. The SA process shall proceed according to the DHS Sensitive Systems Policy Directive 4300A (Version 11.0, April 30, 2014), or any successor publication, DHS 4300A Sensitive Systems Handbook (Version 9.1, July 24, 2012), or any successor publication, and the Security Authorization Process Guide including templates.

Security Authorization Process Documentation. SA documentation shall be developed using the Government provided Requirements Traceability Matrix and Government security documentation templates. SA documentation consists of the following: Security Plan, Contingency Plan, Contingency Plan Test Results, Configuration Management Plan, Security Assessment Plan, Security Assessment Report, and Authorization to Operate Letter. Additional documents that may be required include a Plan(s) of Action and Milestones and Interconnection Security Agreement(s). During the development of SA documentation, the Contractor shall submit a signed SA package, validated by an independent third party, to the COR for acceptance by the Headquarters or Component CIO, or designee, at least thirty (30) days prior to the date of operation of the IT system. The Government is the final authority on the compliance of the SA package and may limit the number of resubmissions of a modified SA package. Once the ATO has been accepted by the Headquarters or Component CIO, or designee, the Contracting Officer shall incorporate the ATO into the contract as a compliance document. The Government's acceptance of the ATO does not alleviate the Contractor's responsibility to ensure the IT system controls are implemented and operating effectively.

Independent Assessment. Contractors shall have an independent third party validate the security and privacy controls in place for the system(s). The independent third party shall review and analyze the SA package, and report on technical, operational, and management level deficiencies as outlined in NIST Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations. The Contractor shall address all deficiencies before submitting the SA package to the Government for acceptance.

Support the completion of the Privacy Threshold Analysis (PTA) as needed. As part of the SA process, the Contractor may be required to support the Government in the completion of the PTA. The requirement to complete a PTA is triggered by the creation, use, modification, upgrade, or disposition of a Contractor IT system that will store, maintain and use PII, and must be renewed at least every three (3) years. Upon review of the PTA, the DHS Privacy Office determines whether a Privacy Impact Assessment (PIA) and/or Privacy Act System of Records Notice (SORN), or modifications thereto, are required. The Contractor shall provide all support necessary to assist the Department in completing the PIA in a timely manner and shall ensure that project management plans and schedules include time for the completion of the PTA, PIA, and SORN (to the extent required) as milestones. Support in this context includes responding timely to requests for information from the Government about the use, access, storage, and maintenance of PII on the Contractor's system, and providing timely review of relevant compliance documents for factual accuracy. Information on the DHS privacy compliance process, including PTAs, PIAs, and SORNs, is accessible at http://www.dhs.gov/privacy-compliance.

(2) Renewal of ATO. Unless otherwise specified in the ATO letter, the ATO shall be renewed every three (3) years. The Contractor is required to update its SA package as part of the ATO renewal process. The Contractor shall update its SA package by one of the following methods:

(1) Updating the SA documentation in the DHS automated information assurance tool for acceptance by the Headquarters or Component CIO, or designee, at least 90 days before the ATO expiration date for review and verification of security controls; or
(2) Submitting an updated SA package directly to the COR for approval by the Headquarters or Component CIO, or designee, at least 90 days before the ATO expiration date for review and verification of security controls. The 90 day review process is independent of the system production date and therefore it is important that the Contractor build the review into project schedules. The reviews may include onsite visits that involve physical or logical inspection of the Contractor environment to ensure controls are in place.

(3) Security Review. The Government may elect to conduct random periodic reviews to ensure that the security requirements contained in this contract are being implemented and enforced. The Contractor shall afford DHS, the Office of the Inspector General, and other Government organizations access to the Contractor's facilities, installations, operations, documentation, databases and personnel used in the performance of this contract. The Contractor shall, through the Contracting Officer and COR, contact the Headquarters or Component CIO, or designee, to coordinate and participate in review and inspection activity by Government organizations external to the DHS. Access shall be provided, to the extent necessary as determined by the Government, 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 Government data or the function of computer systems used in performance of this contract and to preserve evidence of computer crime.

(4) Continuous Monitoring. All Contractor-operated systems that input, store, process, output, and/or transmit sensitive information shall meet or exceed the continuous monitoring requirements identified in the Fiscal Year 2014 DHS Information Security Performance Plan, or successor publication. The plan is updated on an annual basis. The Contractor shall also store monthly continuous monitoring data at its location for a period not less than one year from the date the data is created. The data shall be encrypted in accordance with FIPS 140-2 Security Requirements for Cryptographic Modules and shall not be stored on systems that are shared with other commercial or Government entities. The Government may elect to perform continuous monitoring and IT security scanning of Contractor systems from Government tools and infrastructure.

(5) Revocation of ATO. In the event of a sensitive information incident, the Government may suspend or revoke an existing ATO (either in part or in whole). If an ATO is suspended or revoked in accordance with this provision, the Contracting Officer may direct the Contractor to take additional security measures to secure sensitive information. These measures may include restricting access to sensitive information on the Contractor IT system under this contract. Restricting access may include disconnecting the system processing, storing, or transmitting the sensitive information from the Internet or other networks or applying additional security controls.

(6) Federal Reporting Requirements. Contractors operating information systems on behalf of the Government or operating systems containing sensitive information shall comply with Federal reporting requirements. Annual and quarterly data collection will be coordinated by the Government. Contractors shall provide the COR with requested information within three (3) business days of receipt of the request. Reporting requirements are determined by the Government and are defined in the Fiscal Year 2014 DHS Information Security Performance

Plan, or successor publication. The Contractor shall provide the Government with all information to fully satisfy Federal reporting requirements for Contractor systems.

(f) Sensitive Information Incident Reporting Requirements.

(1) All known or suspected sensitive information incidents shall be reported to the Headquarters or Component Security Operations Center (SOC) within one hour of discovery in accordance with 4300A Sensitive Systems Handbook Incident Response and Reporting requirements. When notifying the Headquarters or Component SOC, the Contractor shall also notify the Contracting Officer, COR, Headquarters or Component Privacy Officer, and US-CERT using the contact information identified in the contract. If the incident is reported by phone or the Contracting Officer's email address is not immediately available, the Contractor shall contact the Contracting Officer immediately after reporting the incident to the Headquarters or Component SOC. The Contractor shall not include any sensitive information in the subject or body of any e-mail. To transmit sensitive information, the Contractor shall use FIPS 140-2 Security Requirements for Cryptographic Modules compliant encryption methods to protect sensitive information in attachments to email. Passwords shall not be communicated in the same email as the attachment. A sensitive information incident shall not, by itself, be interpreted as evidence that the Contractor has failed to provide adequate information security safeguards for sensitive information, or has otherwise failed to meet the requirements of the contract.

(2) If a sensitive information incident involves PII or SPII, in addition to the reporting requirements in 4300A Sensitive Systems Handbook Incident Response and Reporting, Contractors shall also provide as many of the following data elements that are available at the time the incident is reported, with any remaining data elements provided within 24 hours of submission of the initial incident report:

- Data Universal Numbering System (DUNS);
- Contract numbers affected unless all contracts by the company are affected;
- Facility CAGE code if the location of the event is different than the prime contractor location;
- Point of contact (POC) if different than the POC recorded in the System for Award Management (address, position, telephone, email);
- Contracting Officer POC (address, telephone, email);
- Contract clearance level;
- Name of subcontractor and CAGE code if this was an incident on a subcontractor network;
- Government programs, platforms or systems involved;
- Location(s) of incident;
- Date and time the incident was discovered;
- Server names where sensitive information resided at the time of the incident, both at the Contractor and subcontractor level;
- Description of the Government PII and/or SPII contained within the system;
- Number of people potentially affected and the estimate or actual number of records exposed and/or contained within the system; and
- Any additional information relevant to the incident.

(g) Sensitive Information Incident Response Requirements.

All determinations related to sensitive information incidents, including response activities, notifications to affected individuals and/or Federal agencies, and related services (e.g., credit monitoring) will

be made in writing by the Contracting Officer in consultation with the Headquarters or Component CIO and Headquarters or Component Privacy Officer.

The Contractor shall provide full access and cooperation for all activities determined by the Government to be required to ensure an effective incident response, including providing all requested images, log files, and event information to facilitate rapid resolution of sensitive information incidents.

Incident response activities determined to be required by the Government may include, but are not limited to, the following:

- Inspections,
- Investigations,
- Forensic reviews, and
- Data analyses and processing.

The Government, at its sole discretion, may obtain the assistance from other Federal agencies and/or third-party firms to aid in incident response activities.

(h) Additional PII and/or SPII Notification Requirements.

(1) The Contractor shall have in place procedures and the capability to notify any individual whose PII resided in the Contractor IT system at the time of the sensitive information incident not later than 5 business days after being directed to notify individuals, unless otherwise approved by the Contracting Officer. The method and content of any notification by the Contractor shall be coordinated with, and subject to prior written approval by the Contracting Officer, in consultation with the Headquarters or Component Privacy Officer, utilizing the DHS Privacy Incident Handling Guidance. The Contractor shall not proceed with notification unless the Contracting Officer, in consultation with the Headquarters or Component Privacy Officer, has determined in writing that notification is appropriate.

(2) Subject to Government analysis of the incident and the terms of its instructions to the Contractor regarding any resulting notification, the notification method may consist of letters to affected individuals sent by first class mail, electronic means, or general public notice, as approved by the Government. Notification may require the Contractor's use of address verification and/or address location services. At a minimum, the notification shall include:

- A brief description of the incident;
- A description of the types of PII and SPII involved;
- A statement as to whether the PII or SPII was encrypted or protected by other means;
- Steps individuals may take to protect themselves;
- What the Contractor and/or the Government are doing to investigate the incident, to mitigate the incident, and to protect against any future incidents; and
- Information identifying who individuals may contact for additional information.

(i) Credit Monitoring Requirements. In the event that a sensitive information incident involves PII or SPII, the Contractor may be required to, as directed by the Contracting Officer:

Provide notification to affected individuals as described above; and/or

Provide credit monitoring services to individuals whose data was under the control of the Contractor or resided in the Contractor IT system at the time of the sensitive information incident for a period beginning the date of the incident and extending not less than 18 months from the date the individual is notified. Credit monitoring services shall be provided from a company with which the Contractor has no affiliation. At a minimum, credit monitoring services shall include:

- Triple credit bureau monitoring;
- Daily customer service;

- Alerts provided to the individual for changes and fraud; and
- Assistance to the individual with enrollment in the services and the use of fraud alerts; and/or
- Establish a dedicated call center.

Call center services shall include:

- A dedicated telephone number to contact customer service within a fixed period;
- Information necessary for registrants/enrollees to access credit reports and credit scores;
- Weekly reports on call center volume, issue escalation (i.e., those calls that cannot be handled by call center staff and must be resolved by call center management or DHS, as appropriate), and other key metrics;
- Escalation of calls that cannot be handled by call center staff to call center management or DHS, as appropriate;
- Customized FAQs, approved in writing by the Contracting Officer in coordination with the Headquarters or Component Chief Privacy Officer; and
- Information for registrants to contact customer service representatives and fraud resolution representatives for credit monitoring assistance.

(j) Certification of Sanitization of Government and Government-Activity-Related Files and Information. As part of contract closeout, the Contractor shall submit the certification to the COR and the Contracting Officer following the template provided in NIST Special Publication 800-88 Guidelines for Media Sanitization.

(End of Clause)

Information Technology Security and Privacy Training (Mar 2015)

(a) Applicability. This clause applies to the Contractor, its subcontractors, and Contractor employees (hereafter referred to collectively as "Contractor"). The Contractor shall insert the substance of this clause in all subcontracts.

(b) Security Training Requirements.

(1) All users of Federal information systems are required by Title 5, Code of Federal Regulations, Part 930.301, Subpart C, as amended, to be exposed to security awareness materials annually or whenever system security changes occur, or when the user's responsibilities change. The Department of Homeland Security (DHS) requires that Contractor employees take an annual Information Technology Security Awareness Training course before accessing sensitive information under the contract. Unless otherwise specified, the training shall be completed within thirty (30) days of contract award and be completed on an annual basis thereafter not later than October 31st of each year. Any new Contractor employees assigned to the contract shall complete the training before accessing sensitive information under the contract. The training is accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors. The Contractor shall maintain copies of training certificates for all Contractor and subcontractor employees as a record of compliance. Unless otherwise specified, initial training certificates for each Contractor and subcontractor employee shall be provided to the Contracting Officer's Representative (COR) not later than thirty (30) days after contract award. Subsequent training certificates to satisfy the annual training requirement shall be submitted to the COR via e-mail notification not later than October 31st of each year. The e-mail notification shall state the required training has been completed for all Contractor and subcontractor employees.

(2) The DHS Rules of Behavior apply to every DHS employee, Contractor and subcontractor that will have access to DHS systems and sensitive information. The DHS Rules of Behavior shall be signed before accessing DHS systems and sensitive information. The DHS Rules of Behavior is a document that informs users of their responsibilities when accessing DHS systems and holds users accountable for actions taken while accessing DHS systems and using DHS Information Technology resources capable of inputting, storing, processing, outputting, and/or transmitting sensitive information. The DHS Rules of Behavior is accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors. Unless otherwise specified, the DHS Rules of Behavior shall be signed within thirty (30) days of contract award. Any new Contractor employees assigned to the contract shall also sign the DHS Rules of Behavior before accessing DHS systems and sensitive information. The Contractor shall maintain signed copies of the DHS Rules of Behavior for all Contractor and subcontractor employees as a record of compliance. Unless otherwise specified, the Contractor shall e-mail copies of the signed DHS Rules of Behavior to the COR not later than thirty (30) days after contract award for each employee. The DHS Rules of Behavior will be reviewed annually and the COR will provide notification when a review is required.

(c) Privacy Training Requirements. All Contractor and subcontractor employees that will have access to Personally Identifiable Information (PII) and/or Sensitive PII (SPII) are required to take Privacy at DHS: Protecting Personal Information before accessing PII and/or SPII. The training is accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors. Training shall be completed within thirty (30) days of contract award and be completed on an annual basis thereafter not later than October 31st of each year. Any new Contractor employees assigned to the contract shall also complete the training before accessing PII and/or SPII. The Contractor shall maintain copies of training certificates for all Contractor and subcontractor employees as a record of compliance. Initial training certificates for each Contractor and subcontractor employee shall be provided to the COR not later than thirty (30) days after contract award. Subsequent training certificates to satisfy the annual training requirement shall be submitted to the COR via e-mail notification not later than October 31st of each year. The e-mail notification shall state the required training has been completed for all Contractor and subcontractor employees.

(End of Clause)

PART III - List of Documents, Exhibits, and Attachments

Attachment(s):

A. Performance Work Statement, 6 Pages

Department of Homeland Security
US Citizenship and Immigration Services
Behavioral Threat Assessment, Consultation & Training Services
Performance Work Statement

1.0 Background

US Citizenship and Immigration Services (USCIS) is establishing a new agency-wide Workplace Violence Prevention Program, to include domestic violence, sexual assault and stalking affecting the workplace. The program incorporates the use of five specially trained multi-disciplinary threat assessment and management units, or Situational Advisory Teams (SATs). SATs are trained to intake and manage violence risk cases internal to an organization of approximately 32,000 personnel. SATs are comprised of personnel from the following disciplines: security, legal counsel, and employee relations.

In anticipation of receiving specialized cases needing external consultation, USCIS seeks a tailored consultation from an external behavioral threat assessment professional(s), administrative analytical support, and annual training of SAT personnel in customized areas of threat assessment and management.

Compliment to the Workplace Violence Prevention Program is the Personnel Security program, which continuously vets employee and contractor suitability and clearances. USCIS also requires assistance with its personnel security program and as part of this requirement is seeking comprehensive psychological consultation for suitability and clearance determinations.

2.0 Scope

The purpose of this contract is to provide USCIS with a qualified behavioral threat assessment professional to consult on challenging violence risk cases upon request, to deliver annual training to SAT personnel, and to provide consultation for suitability and clearance determinations.

3.0 Period of Performance

The period of performance for this requirement is 3 years (One 12-month base and two 12-month options).

4.0 Place of Performance

The contractor shall perform a majority of the work at its own facility. However, the contractor may be required to travel to a location specified by the government to conduct further in-person consultations or evaluations on a case-by-case basis. Training shall be performed at USCIS locations. See section 5.3.2.

5.0 Tasks

5.1 Behavioral Threat Assessment

5.1.1 Specific Task Requirements:

The contractor must be available for consultation within 6 hours of initial consultation request. The contractor shall perform:

5.1.1.1 Initial Behavioral Threat Assessment Consultation (Consultation) – the initial request for consultation will be communicated to the contractor via email or telephone and the contractor shall respond within 6 hours.

The contractor shall perform the following, as determined necessary based on the initial consultation:

5.1.1.2 Information evaluation – Contractor shall work with Contracting Officer's Representative (COR) to determine estimated number of hours to complete case, based on known information.

5.1.1.3 Behavioral threat assessment case strategy and management plan– Contractor shall evaluate case information and draw a written behavioral threat assessment and analysis, outlining behavioral risk factors correlating to levels of concern, methodology and rationale for analysis, and recommendations on managing or mitigating behaviors of concern for USCIS employees and/or contractors involved in the situation of concern.

5.1.1.4 Informational Briefings – Contractor shall provide informational briefings to stakeholders/customers on case developments, assessment, recommendations, and outcomes.

5.2 Personnel Security Evaluations

5.2.1 Contractor shall evaluate personnel security information, reviewing all available information, and directly examine USCIS employees or contractors for psychological, diagnostic assessment and personality functioning.

5.2.2 Contractor shall write conclusion to report with clear findings that have investigative and adjudicative utility and address trustworthiness, reliability and judgment. Within 10 days of the initial request, submit report to requesting agency through a secure portal.

5.2.3 If necessary, the contractor shall review report findings with requestor and edit report to provide clarification, and then resubmit report if changes have been made.

5.3 Training

5.3.1 Specific Training Task Requirements:

The contractor shall develop and hold one**,** two (2)-day training during the base year for up to 150 Situational Advisory Team (SAT) personnel (50 in person and 100 virtual attendance). Contractor shall provide one, two (2)-day training at multiple locations during the Option years for up to thirty (30) personnel per site. Specific dates and locations will be established after award. USCIS will provide the contractor a two-week notice via the Contracting Officer if a training is to be cancelled or rescheduled at no expense to USCIS.

USCIS will have personnel escort the instructor(s) for the duration of the seminars.

The training shall be customized for members of SATs physically and virtually attending the training. Over the entire period of performance of the contract, the training shall cover the following topics as related to threat assessment and management:

(1) Threat assessment and management,
(2) Managing victim fear,
(3) Management strategies for subjects,

(4) Analysis of anonymous threat communications,
(5) Domestic Violence, Sexual Assault, and Stalking,
(6) Suicide, as related to threat assessment
(7) Legal considerations in threat assessment
(8) Information gathering,
(9) Interviewing strategies & practical exercises, and
(10) Tabletop case studies.

ii) Each training shall include at minimum:

(1) training plan curriculum (agenda),
(2) training materials deemed as appropriate, and
(3) references and illustrations for the training materials.

iii) Contractor shall provide hard copies for each attendee and electronic copy to the COR.

iv) Each stage of the SAT training will require approval from the Program Manager (PM) or Associate Program Manager (APM) for Workplace Violence Prevention and COR through informational briefings. Prior to training delivery, the vendor shall consult via conference call (or in person if contractor is local) with the PM or APM to develop a training curriculum tailored for USCIS. The draft curriculum shall require approval 60 days in advance of the training, and the final curriculum shall require approval 30 days in advance of the training. No changes to the curriculum shall be made without the approval of the Workplace Violence Program Manager. In addition, one month prior to training delivery, the contractor shall meet weekly with the PM or APM for training preparation meetings and/or as needed via email or conference call.

v) Training may be recorded.

vi) Contractor instructor(s) shall be familiar with equipment in classroom ahead of time, and shall conduct the training with professionalism (i.e. Neat in appearance, proper demeanor, reliable, competent, good communicator, poised).

vii) Contractor shall present a training evaluation survey to attendees;

viii) After the training delivery, Contractor shall create, and present to PM and COR for review and approval, an after action report, with evaluation survey results, analysis, and recommendations for future training.

5.3.2 Training Locations

Training for the base year shall be provided in Washington, DC.
Training locations for both Option Years are as follows. Training cities will not change, but training location addresses may be subject to change, and will be finalized with vendor during training planning stage:

Washington, DC: 111 Massachusetts Avenue, Washington, D.C.
OR 1 Town Center, Camp Springs, MD

Burlington, VT: 237 Harvest Lane, Williston, VT 05495

Orlando, FL: 390 North Orange Avenue, Suite 1943, Orlando, FL 32801

Dallas, TX: 4500 Fuller Drive, Irving, TX 75038
Minneapolis, MN: 9360 Ensign Ave South; Bloomington MN 55438

Laguna Niguel, CA: 24000 Avila Road, Laguna Niguel, CA 92677

6.0 Personnel Requirements

6.1 Behavioral Threat Assessment and Training.

6.1.1. Senior Consultant. The contractor's senior consultant for behavioral risk evaluations and training shall have, at minimum, the following qualifications:

a. Minimum of 10 years case consultation experience;
b. Minimum of 5 years of experience in training delivery of behavioral threat assessment and management;
c. Experience and use of adult learning styles and techniques in training format;
d. Experience and use of styles and techniques for virtual learning environment;
e. Shall have knowledge of criminal, civil, and employment law;
f. Contractor shall provide all applicable credentials (such as education or certifications) for qualification of behavioral threat assessment consultation work. Specifically, the contractor delivering behavioral threat assessment consultation shall possess a degree (PhD or PsyD) as a clinical psychologist and at least 10 years' experience in violence risk assessment, threat assessment, and threat management.

6.1.2 Legal and Investigative Personnel. The Contractor shall also be able to supply, if warranted, personnel for legal and investigative expertise as pertaining to threat assessment and management, with 5 or more years' experience in violence risk assessment, threat assessment and threat management.

6.2 Security Evaluations: The contractor's senior consultant for personnel security evaluations shall have, at minimum, the following required qualifications:

a. Be a licensed psychologist (PhD/PsyD) and/or board-certified psychiatrist to assist in the personnel security vetting process.
b. Have experience conducting independent review and adjudication of medical documentation, diagnosis and analysis for agency decision-making on personnel adjudications and clearance holders.

7.0 Travel

Travel is required to conduct the trainings at the designated USCIS offices. Travel for in-person direct behavioral risk evaluations may be required upon request. The contractor shall be responsible for obtaining Contracting Officer's Representative (COR) approval (electronic mail is acceptable) for all reimbursable travel in advance of booking the travel event. The rates (per diem, personal vehicle mileage, etc.) at which the contractor will be reimbursed for travel necessary for performance under this contract shall be no greater than those allowed by Federal Travel Regulations, current as of the time the travel occurs in accordance with FAR 31.205-46, Travel Costs. The contractor shall be responsible for making their own travel arrangements.

8.0 Deliverables

Deliverable Description	References	Format	Deliver To	Due Date
Initial Behavioral Threat Assessment Consultation	Task 5.1.1.1	E-mail or conference call	Program Manager (PM)/ Associate Program Manager (APM)	Within 6 hours after consultation request
Information evaluation	Task 5.1.1.2	E-mail or conference call	PM/ APM	TBD with PM/APM or alternate per instance
Case strategy recommendations	Task 5.1.1.3	Document in MS Word or Excel (2016 or later)	PM/ APM	5 business days from case assessment
Behavioral threat assessment and management plan	Task 5.1.1.4	Document in MS Word or Excel (2016 or later)	PM/ APM	10 business days from completion of behavioral risk evaluation
Personnel security assessment	Task 5.2	Document, in MS Word or Excel (2016 or later)	Personnel Security Adjudicator PM/APM	10 business days from request
Informational briefings - Contractor's leadership and/or technical experts shall be available to provide informational briefings.	Task 5.1.1.4	Conference call; in-person, as applicable	PM/ APM	Exact dates TBD with and PM /APM
Training: Curriculum	Task 5.3.1 (ii)	Document, in MS Word or Excel (2016 or later)	PM/APM	60 days prior to training delivery
Training: The contractor shall develop and hold a 2-day training during base year and 2-day training at 6 locations annually thereafter.	Task 5.3.1	In-house	SAT/PM	Exact dates TBD with PM / APM
Training: After Action Report	Task 5.3.1. (vii)	Document, in MS Word or Excel	PM/APM	Within 30 days after training delivery

		(2016 or later)		

9.0 Performance Standards

The contract Quality Assurance Surveillance Plan (QASP) will be used to monitor performance. The contractor shall meet with the PM/APM and COR on or before the 25th calendar day of each month to review and discuss contractor personnel performance.

Performance standards (unless otherwise specified):

- Performance – Deliverables fully coordinated among stakeholders; efforts enhance USCIS HCT objectives;
- Timeliness – Meets required deadlines or schedules as outlined in the deliverables table; documentation is submitted to the Government in sufficient time for review and approval;
- Quality – Deliverables based on properly coordinated efforts; deliverables produced in the Government Requestor approved format; technically and factually correct; accurate, complete and free of grammatical, typographical and spelling errors; satisfies intended purpose.