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

1. REQUISITION NUMBER: OIT173010/173030/175016

PAGE 1 OF 57

2. CONTRACT NO.: HSHQDC-13-D-E2075

3. AWARD/EFFECTIVE DATE: 08/02/17

4. ORDER NUMBER: HSSCCG-17-J-00086

5. SOLICITATION NUMBER: HSSCCG-17-R-00020

6. SOLICITATION ISSUE DATE: 05/19/2017

7. FOR SOLICITATION INFORMATION CALL: a. NAME: Stuart Sellears; b. TELEPHONE NUMBER *(No collect calls)*: 802-872-4111

8. OFFER DUE DATE/LOCAL TIME:

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: 518210
SIZE STANDARD: $30.0

11. DELIVERY FOR FOB DESTINATION UNLESS BLOCK IS MARKED ☐ SEE SCHEDULE

12. DISCOUNT TERMS: Net 30

13a. ☐ THIS CONTRACT IS A RATED ORDER UNDER DPAS (15 CFR 700)

13b. RATING:

14. METHOD OF SOLICITATION: ☐ RFQ ☐ IFB ☐ RFP

15. DELIVER TO — CODE: HQOIT

Department of Homeland Security
US Citizenship & Immigration Svcs
Office of Information Technology
111 Massachusetts Ave, NW
Suite 5000
Washington DC 20529

16. ADMINISTERED BY — CODE: CIS

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

17a. CONTRACTOR/OFFEROR — CODE: 1325996680000 — FACILITY CODE:

SEVATEC INC
3112 FAIRVIEW PARK DRIVE
FALLS CHURCH VA 220424504

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: 132599668+0000 Cyber Security Cyber Defense Services (CSDS) This order is subject to the terms and conditions of the EAGLE II contract HSHQDC-13-D-E2075. Contract Type: Time and Materials The task order will begin after issuance of the notice to proceed (NTP). After issuance of the transition NTP there will be approximately a				

(Use Reverse and/or Attach Additional Sheets as Necessary)

25. ACCOUNTING AND APPROPRIATION DATA: See schedule

26. TOTAL AWARD AMOUNT *(For Govt. Use Only)*: [redacted]

☐ 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 ____________ 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: Sevatec Proposal OFFER DATED 08/09/2017. 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: [redacted]

30b. NAME AND TITLE OF SIGNER *(Type or print)*: [redacted]

30c. DATE SIGNED: [redacted]

31a. UNITED STATES OF AMERICA *(SIGNATURE OF CONTRACTING OFFICER)*: Nacole Greenwood

31b. NAME OF CONTRACTING OFFICER *(Type or print)*: Nacole Greenwood

31c. DATE SIGNED: 8/2/17

AUTHORIZED FOR LOCAL REPRODUCTION
PREVIOUS EDITION IS NOT USABLE

19. ITEM NO.	20. SCHEDULE OF SUPPLIES/SERVICES	21. QUANTITY	22. UNIT	23. UNIT PRICE	24. AMOUNT
	2-month transition period, followed by a 10-month base period, and two 12 month option periods. Please note that the Enter-On-Duty (EOD) process shall begin immediately following award of this task order. AAP Number: None DO/DPAS Rating: NONE Period of Performance: 09/04/2017 to 09/03/2018				
0001	Transition-In as detailed in SOW section 5.5 Not to Exceed [redacted] Accounting Info: ITSECN0 FMS EX 20-01-00-000 23-20-0300-00-00-00-00 GE-25-76-00 000000 Funded: [redacted] Accounting Info: ITSECN0 FMS EP 20-05-00-000 23-20-0500-00-00-00-00 GE-25-76-00 000000 Funded: [redacted] Accounting Info: ITISDNL 000 EX 20-01-00-000 23-20-0300-00-00-00-00 GE-31-15-00 000000 Funded: [redacted]	[redacted]	[redacted]	[redacted]	[redacted]
0002	Program Management and Project Planning as detailed in SOW sections 3.1 and 4.2 Accounting Info: ITSECN0 FMS EX 20-01-00-000 Continued ...	[redacted]	[redacted]	[redacted]	[redacted]

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

41b. SIGNATURE AND TITLE OF CERTIFYING OFFICER

41c. DATE

42a. RECEIVED BY *(Print)*

42b. RECEIVED AT *(Location)*

42c. DATE REC'D *(YY/MM/DD)*

42d. TOTAL CONTAINERS

NAME OF OFFEROR OR CONTRACTOR
SEVATEC INC

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	23-20-0300-00-00-00-00 GE-25-76-00 000000 Funded: [redacted] Accounting Info: ITSECN0 FMS EP 20-05-00-000 23-20-0500-00-00-00-00 GE-25-76-00 000000 Funded: [redacted]				
0003	Labor Hours Accounting Info: ITSECN0 FMS EX 20-01-00-000 23-20-0300-00-00-00-00 GE-25-76-00 000000 Funded: [redacted] Accounting Info: ITSECN0 FMS EP 20-05-00-000 23-20-0500-00-00-00-00 GE-25-76-00 000000 Funded: [redacted]	[redacted]	[redacted]	[redacted]	[redacted]
0003 AA	Not Separately Priced - Detecting Security Incidents as detailed in SOW sections 3.2 and 4.3 (Not Separately Priced) Accounting Info: Funded: [redacted]		[redacted]	[redacted]	[redacted]
0003 AB	Not Separately Priced - Assessing Security through Exercises, Assessments, and Penetration Testing as detailed in SOW sections 3.3 and 4.4 (Not Separately Priced) Accounting Info: Funded: [redacted]		[redacted]	[redacted]	[redacted]
0003 AC	Not Separately Priced - Developing Secure Code as detailed in SOW sections 3.4 and 4.5 (Not Separately Priced) Accounting Info: Funded: [redacted]		[redacted]	[redacted]	[redacted]
0003 AD	Not Separately Priced - Securing the Network as detailed in SOW sections 3.5 and 4.6 (Not Separately Priced) Accounting Info: Funded: [redacted] Continued ...		[redacted]	[redacted]	[redacted]

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
0003 AE	Not Separately Priced - Maintaining Security Hygiene, Supporting Enterprise Security Engineering, and Developing Enterprise Security Solutions as detailed in SOW sections 3.6, 3.8, 3.9, and 4.7 (Not Separately Priced) Accounting Info: Funded: [redacted]		[redacted]	[redacted]	[redacted]
0003 AF	Not Separately Priced - Implementing the Continuous Diagnostics and Monitoring Program as detailed in SOW sections 3.7 and 4.8 (Not Separately Priced) Accounting Info: Funded: [redacted]		[redacted]	[redacted]	[redacted]
0003 AG	Not Separately Priced - Securing the Cloud as detailed in SOW sections 3.10 and 4.9 (Not Separately Priced) Accounting Info: Funded: [redacted]		[redacted]	[redacted]	[redacted]
0004	Travel/Other Direct Costs (ODC) (Not to Exceed) Accounting Info: ITSECN0 FMS EP 20-05-00-000 23-20-0500-00-00-00-00 GE-25-76-00 000000 Funded: [redacted] Accounting Info: ITSECN0 FMS EX 20-01-00-000 23-20-0300-00-00-00-00 GE-25-76-00 000000 Funded: [redacted]	[redacted]	[redacted]	[redacted]	[redacted]
1002	Program Management and Project Planning as detailed in SOW sections 3.1 and 4.2 Amount: [redacted] Anticipated Exercise Date:08/03/2018	[redacted]	[redacted]	[redacted]	[redacted]
1003	Labor Hours Amount: [redacted] Anticipated Exercise Date:08/03/2018	[redacted]	[redacted]	[redacted]	[redacted]
	Continued ...				

CONTINUATION SHEET	REFERENCE NO. OF DOCUMENT BEING CONTINUED HSHQDC-13-D-E2075/HSSCCG-17-J-00086	PAGE	OF
		5	57

NAME OF OFFEROR OR CONTRACTOR
SEVATEC INC

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
1003 AA	Not Separately Priced - Detecting Security Incidents as detailed in SOW sections 3.2 and 4.3 Amount: [redacted](Option Line Item) Anticipated Exercise Date:08/03/2018 (Not Separately Priced)		[redacted]	[redacted]	[redacted]
1003 AB	Not Separately Priced - Assessing Security through Exercises, Assessments, and Penetration Testing as detailed in SOW sections 3.3 and 4.4 Amount: [redacted](Option Line Item) Anticipated Exercise Date:08/03/2018 (Not Separately Priced) Accounting Info: Funded: [redacted]		[redacted]	[redacted]	[redacted]
1003 AC	Not Separately Priced - Developing Secure Code as detailed in SOW sections 3.4 and 4.5 Amount: [redacted](Option Line Item) Anticipated Exercise Date:08/03/2018 (Not Separately Priced) Accounting Info: Funded: [redacted]		[redacted]	[redacted]	[redacted]
1003 AD	Not Separately Priced - Securing the Network as detailed in SOW sections 3.5 and 4.6 Amount: [redacted](Option Line Item) Anticipated Exercise Date:08/03/2018 (Not Separately Priced) Accounting Info: Funded: [redacted]		[redacted]	[redacted]	[redacted]
1003 AE	Not Separately Priced - Maintaining Security Hygiene, Supporting Enterprise Security Engineering, and Developing Enterprise Security Solutions as detailed in SOW sections 3.6, 3.8, 3.9, and 4.7 Amount: [redacted](Option Line Item) Anticipated Exercise Date:08/03/2018 (Not Separately Priced)		[redacted]	[redacted]	[redacted]
1003 AF	Not Separately Priced - Implementing the Continuous Diagnostics and Monitoring Program as Continued ...		[redacted]	[redacted]	[redacted]

NAME OF OFFEROR OR CONTRACTOR
SEVATEC INC

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	detailed in SOW sections 3.7 and 4.8 Amount: [redacted](Option Line Item) Anticipated Exercise Date:08/03/2018 (Not Separately Priced)				
1003 AG	Not Separately Priced - Securing the Cloud as detailed in SOW sections 3.10 and 4.9 Amount: [redacted](Option Line Item) Anticipated Exercise Date:08/03/2018 (Not Separately Priced)		[redacted]	[redacted]	[redacted]
1004	Travel/Other Direct Costs (ODC) (Not to Exceed) Amount: [redacted]Option Line Item) Anticipated Exercise Date:08/03/2018	[redacted]	[redacted]	[redacted]	[redacted]
2002	Program Management and Project Planning as detailed in SOW sections 3.1 and 4.2 Amount: [redacted](Option Line Item) Anticipated Exercise Date:08/03/2019	[redacted]	[redacted]	[redacted]	[redacted]
2003	Labor Hours Amount: [redacted](Option Line Item) Anticipated Exercise Date:08/03/2019	[redacted]	[redacted]	[redacted]	[redacted]
2003 AA	Not Separately Priced - Detecting Security Incidents as detailed in SOW sections 3.2 and 4.3 Amount: [redacted](Option Line Item) Anticipated Exercise Date:08/03/2019 (Not Separately Priced)		[redacted]		[redacted]
2003 AB	Not Separately Priced - Assessing Security through Exercises, Assessments, and Penetration Testing as detailed in SOW sections 3.3 and 4.4 Amount: [redacted](Option Line Item) Anticipated Exercise Date:08/03/2019 (Not Separately Priced)		[redacted]		[redacted]
2003 AC	Not Separately Priced - Developing Secure Code as detailed in SOW sections 3.4 and 4.5 Amount: [redacted]Option Line Item) Continued ...		[redacted]		[redacted]

NAME OF OFFEROR OR CONTRACTOR
SEVATEC INC

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	Anticipated Exercise Date:08/03/2019 (Not Separately Priced)				
2003 AD	Not Separately Priced - Securing the Network as detailed in SOW sections 3.5 and 4.6 Amount: [redacted]Option Line Item) Anticipated Exercise Date:08/03/2019 (Not Separately Priced)		[redacted]		[redacted]
2003 AE	Not Separately Priced - Maintaining Security Hygiene, Supporting Enterprise Security Engineering, and Developing Enterprise Security Solutions as detailed in SOW sections 3.6, 3.8, 3.9, and 4.7 Amount: [redacted](Option Line Item) Anticipated Exercise Date:08/03/2019 (Not Separately Priced)		[redacted]		[redacted]
2003 AF	Not Separately Priced - Implementing the Continuous Diagnostics and Monitoring Program as detailed in SOW sections 3.7 and 4.8 Amount: [redacted](Option Line Item) Anticipated Exercise Date:08/03/2019 (Not Separately Priced)		[redacted]		[redacted]
2003 AG	Not Separately Priced - Securing the Cloud as detailed in SOW sections 3.10 and 4.9 Amount: [redacted](Option Line Item) Anticipated Exercise Date:08/03/2019 (Not Separately Priced)		[redacted]		[redacted]
2004	Travel/Other Direct Costs (ODC) (Not to Exceed) Amount: [redacted](Option Line Item) Anticipated Exercise Date:08/03/2019 List of Attachments: 1. Clauses 2. Statement of Work 3. Security Requirements - Security Clause 2S 4. Safeguarding of Sensitive Information 5. Information Technology Security and Privacy Training Continued ...	[redacted]	[redacted]	[redacted]	[redacted]

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)

6. Accessibility Requirements (section 508)

USCIS COR Karen Walton
Email: Karen.N.Walton@uscis.dhs.gov
Phone: (202)272-9844

USCIS Contract Specialist Stuart Sellears
Email: Stuart.Sellears@uscis.dhs.gov
Phone: (802)872-4165

USCIS Contracting Officer Charles Julian
Email: Charles.E.Julian@uscis.dhs.gov
Phone: (802)872-4667

The total amount of award: [redacted]. The obligation for this award is shown in box 26.

TASK ORDER CLAUSES

All applicable terms, conditions and clauses contained in the DHS EAGLE II Functional Category 1 8(a) Master IDIQ Contract apply. Additional clauses are listed below.

FAR CLAUSES INCORPORATED BY REFERENCE

52.209-10	**Prohibition on Contracting with Inverted Domestic Corporations**	(Nov 2015)
52.224-3	**Privacy Training (Alt I)**	(Jan 2017)
52.227-17	**Rights in Data—Special Works**	(Dec 2007)
52.232-7	**Payments under Time-and-Materials and Labor-Hour Contracts**	(Aug 2012)
52.232-39	**Unenforceability of Unauthorized Obligations**	(Jun 2013)
52.237-3	**Continuity of Services**	(Jan 1991)

FAR CLAUSES INCORPORATED IN FULL TEXT

52.203-19 **Prohibition on Contracting with Entities that Require Certain Internal Confidentiality Agreements** (Jan 2017)

(a) Definitions. As used in this clause--

“Internal confidentiality agreement or statement” means a confidentiality agreement or any other written statement that the contractor requires any of its employees or subcontractors to sign regarding nondisclosure of contractor information, except that it does not include confidentiality agreements arising out of civil litigation or confidentiality agreements that contractor employees or subcontractors sign at the behest of a Federal agency.

“Subcontract” means any contract as defined in subpart 2.1 entered into by a subcontractor to furnish supplies or services for performance of a prime contract or a subcontract. It includes but is not limited to purchase orders, and changes and modifications to purchase orders.

“Subcontractor” means any supplier, distributor, vendor, or firm (including a consultant) that furnishes supplies or services to or for a prime contractor or another subcontractor.

(b) The Contractor shall not require its employees or subcontractors to sign or comply with internal confidentiality agreements or statements prohibiting or otherwise restricting such employees or subcontractors from lawfully reporting waste, fraud, or abuse related to the performance of a Government contract to a designated investigative or law enforcement representative of a Federal department or agency authorized to receive such information (e.g., agency Office of the Inspector General).

(c) The Contractor shall notify current employees and subcontractors that prohibitions and restrictions of any preexisting internal confidentiality agreements or statements covered by this clause, to the extent that such prohibitions and restrictions are inconsistent with the prohibitions of this clause, are no longer in effect.

(d) The prohibition in paragraph (b) of this clause does not contravene requirements applicable to Standard Form 312 (Classified Information Nondisclosure Agreement), Form 4414 (Sensitive Compartmented Information Nondisclosure Agreement), or any other form issued by a Federal department or agency governing the nondisclosure of classified information.

(e) In accordance with 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) use of funds appropriated (or otherwise made available) is prohibited, if the Government determines that the Contractor is not in compliance with the provisions of this clause.

(f) The Contractor shall include the substance of this clause, including this paragraph (f), in subcontracts under such contracts.

(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 **15 days of the end of the current period of performance**; provided that the government gives the contractor a preliminary written notice of its intent to extend at least **60 days** before the task order 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)

52.252-4 **Alterations in Contract** (Apr 1984)

Portions of this contract are altered as follows:

Use of the word “contract” is understood to mean “task order” whenever such application is appropriate.

HSAR CLAUSES INCORPORATED IN BY REFERENCE

3052.205-70 **Advertisements, Publicizing Awards, and Releases** (Sep 2012)

Note: The full text of HSAR clauses may be accessed electronically at the following address: http://farsite.hill.af.mil/VFHSAR1.HTM

HSAR CLAUSES INCORPORATED IN FULL TEXT

3052.204-71 – **Contractor Employee Access** (Sept 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)

3052.215-70 **Key Personnel or Facilities** (Dec 2003)

(a) The personnel or facilities specified below are considered essential to the work being performed under this contract and may, with the consent of the contracting parties, be changed from time to time during the course of the contract by adding or deleting personnel or facilities, as appropriate.

(b) Before replacing any of the specified individuals or facilities, the contractor shall notify the contracting officer, in writing, before the change becomes effective. The contractor shall submit sufficient information to support the proposed action and to enable the contracting officer to evaluate the potential impact of the change on this contract. The contractor shall not replace personnel or facilities until the contracting officer approves the change.

The Key Personnel under this contract are:

Program Manager
Sr. Splunk Engineer
Sr. Penetration Tester
Network Engineer Level III
Sr. Security Tools Engineer (Security Engineer III)

(End of clause)

OTHER TASK ORDER REQUIREMENTS

Additional Invoicing Instructions

(a) In accordance with FAR Part 32.905, all invoices submitted to USCIS for payment shall include the following:

(1) Name and address of the contractor.

(2) Invoice date and invoice number.

(3) Contract number or other authorization for supplies delivered or services performed (including order number and contract line item number).

(4) Description, quantity, unit of measure, period of performance, unit price, and extended price of supplies delivered or services performed.

(5) Shipping and payment terms.

(6) Name and address of contractor official to whom payment is to be sent.

(7) Name (where practicable), title, phone number, and mailing address of person to notify in the event of a defective invoice.

(8) Taxpayer Identification Number (TIN).

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

(c) 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 to **USCISInvoice.Consolidation@ice.dhs.gov** with each email conforming to a size limit of 500 KB.

(d) If a paper invoice is submitted, mail the invoice to:

USCIS Invoice Consolidation
PO Box 1000
Williston, VT 05495

Performance Reporting

The government intends to record and maintain contractor performance information for this task order in accordance with FAR Subpart 42.15. The contractor is encouraged to enroll at www.cpars.gov so it can participate in this process.

Final Payment

As a condition precedent to final payment, a release discharging the government, its officers, agents and employees of and from all liabilities, obligations, and claims arising out of or under this contract shall be completed. A release of claims will be forwarded to the contractor at the end of each performance period for contractor completion as soon thereafter as practicable.

Government-Furnished Property

(a) Upon the contractor's request that a contractor employee be granted access to a government automated system and the government's approval of the request, the government will issue the following equipment to that employee by hand receipt:

Equipment	**Unit Cost**
Laptop computer	$ 2,500
Apple MacBook	$ 4,000

(b) The contractor is responsible for all costs related to making this equipment available for use, such as payment of all transportation costs. The contractor bears full responsibility for any and all loss of this equipment, whether accidental or purposeful, at full replacement value.

(c) This equipment will be provided on a rent-free basis for performance under this contract (or task order). It shall not be used for any non-contract or non-governmental purpose. The contractor shall ensure the return of the equipment immediately upon the demand of the contracting officer or the end of contract (or task order) performance.

(d) A contractor request may be for a subcontractor employee. If so, the contractor retains all the responsibilities of this clause for equipment issued to that employee.

Notice to Proceed (NTP)

(a) Performance of the work requires unescorted access to government facilities or automated systems, and/or access to sensitive but unclassified information. The Attachment titled Security Requirements applies.

(b) The contractor is responsible for submitting packages for employees who will receive favorable Entry-On-Duty (EOD) decisions and suitability determinations, and for submitting them in a timely manner. A government decision not to grant a favorable EOD decision or suitability determination, or to later withdraw or terminate such, shall not excuse the contractor from performance of its obligations under this task order.

(c) The contractor shall submit background investigation packages immediately following task order award.

(d) This task order does not provide for direct payment to the contractor for EOD efforts. Work for which direct payment is not provided is a subsidiary obligation of the contractor.

(e) The government intends for the transition-in CLIN to begin approximately 30 days after the task order award. The contracting officer will issue a transition notice to proceed (NTP) at least one day before transition is to begin.

(f) The transition-in period shall last for no more than 60 days. Successful completion of the transition period shall occur prior to any notice to proceed with full performance. The contracting officer will issue a full performance NTP at least one day before full performance is to begin.

T&M Ceiling Price

For each T&M CLIN, to include obligated CLINs and optional CLINs, the unit price represents the ceiling price for that CLIN. All terms and conditions affecting ceiling price are understood to apply at the CLIN level. If the offeror exceeds ceiling price, they do so at their own risk.

Posting of Contract (or Order) in FOIA Reading Room

(a) The government intends to post the contract (or 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 contract (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.

Cyber Security Defense Services (CSDS) Statement of Work (SOW)

Start Secure. Stay Secure.

INFORMATIONSECURITY
DIVISION

U.S. Citizenship
and Immigration
Services

Table of Contents

1 Executive Summary

U.S. Citizenship and Immigration Services (USCIS), Office of Information Technology (OIT), Information Security Division (ISD) has a requirement to acquire Cyber Security Defense Services (CSDS) to protect USCIS' IT infrastructure and resources, information systems, and the information used in these environments from cybersecurity threats. The Cyber Defense Branch (CDB) within ISD is responsible for:

- Deploying and operate cyber security tools
- Reviewing USCIS source code
- Assessing the security of USCIS systems and the effectiveness of USCIS security tools and processes through penetration testing and security exercises
- Providing security engineering expertise to other OIT divisions

The scope of this contract includes:

- Security Analytics and Incident Detection
- Penetration Testing and Security Exercise Development
- Secure Code Review
- Network Security
- Enterprise Security Solution Engineering
- Security Engineering support for Agile Development and DevOps

2 Scope: Cyber Defense Requirements

The goal of the Government is to secure IT services supported by an overarching management approach that focuses on the use of Agile processes, technical methods, processes, human resource management techniques and concepts needed to assist the Government in executing and carrying out its IT security mission responsibilities.

The scope of this requirement is for a contractor to perform and execute Cyber Defense activities in accordance with current DHS and USCIS Security Authorization processes and procedures. Congruently, the Contractor shall actively provide documented recommendations (via the monthly status reports) for improving the technical methods and processes.

The nature of the work required by this SOW is episodic and extremely dynamic. The Contractor shall be able to shift workload among the teams, re-organize the team make-up, and shift workload between team members seamlessly. The Contractor shall be able to work seamlessly with other USCIS Contractors and Federal employees as part of cross-functional, cross-organizational Agile DevSecOps teams.

3 Tasks

3.1 Program Management and Project Planning

The Contractor shall assign experienced personnel for program management and project planning. The Contractor’s resources shall possess knowledge and experience with Agile program and project management, and administrative skills for this functional area. The Contractor shall provide program and project management support in the following areas: risk management, integrated schedule management, performance metrics, document management, and change management. In addition, the Contractor shall support the facilitation of effective governance, cross-project integration, performance monitoring and the implementation of Agile security processes.

While the Contractor will have traditional and Agile program management roles and functions, the Contractor's staff may be matrixed to focus on the specific task requirements. Generally, work will be performed at the contractor facility in the National Capital Region (NCR). Some contractor personnel will also be located at USCIS sites in Williston, VT. To facilitate coordination and communication, contractor personnel in the NCR may be required to work from USCIS sites in the NCR on an episodic basis or attend in-person meetings at these sites.

The Contractor Program and Project Managers shall perform the following throughout the life of this task order:

- Apply industry and Government standards and best practices as appropriate in the service areas specified in this SOW.
- Attend weekly status meetings with the Government Program Managers.
- Coordinate quarterly/monthly Program Management Review meetings with Government staff and Contractor management staff.
- Ensure that Agile approaches are established and maintained on the program and associated projects and reflected in the team's approach.
- Ensure Agile measurements of progress such as Kanban boards are used and kept up to date.
- Ensure use of USCIS OIT standard enterprise planning and tracking tools.
- Utilize processes that ensure continuity of operations and smooth transition of the management responsibilities throughout the life of the contract.

3.2 Detecting Security Incidents

Defending the perimeter is not sufficient to stop determined intruders. Rather, organizations must assume that their systems and networks may already be compromised and deploy analytic and anomaly detection capabilities to identify intrusions as early in the intrusion kill chain as possible. The Contractor shall assess, develop, implement, deploy, and operate solutions for capturing security relevant information (e.g. log data, NetFlow data), and analyzing it to identify markers, patterns, and anomalies that indicate intrusions, lateral movement, command and control, data exfiltration, or other security issues. The Contractor shall operate the USCIS Security Information and Event Management (SIEM) tool, and work collaboratively with development and operational teams to set and implement standards for logging.

The Contractor shall:

- Provide DevOps support for a multi-data center, multi-region log management system. The system currently in use is Splunk Enterprise. This support includes, but is not limited to user account and access management, server management, monitoring, and patching, Splunk data management, Splunk version upgrades, installation and maintenance of Splunk applications and add-ons.
- Improve log coverage and quality. This includes:
  - Reconciling records of log sources in Splunk with other asset management data to identify assets whose logs are not in Splunk;
  - Establishing specific logging standards for commonly used software applications and monitoring compliance with the standards;
  - Auditing log content and quality for custom developed USCIS applications; and

  - Automating the production of documentation of the log sources in each Splunk index.
- Provide DevOps support to deploy visualization, analysis, analytics, and anomaly detection capabilities. As directed by the government, the Contractor shall:
  - Evaluate, deploy, and operate visualization, security analysis, and anomaly detection capabilities;
  - Deploy and operate Exabeam Threat Hunter;
  - Implement machine learning in Splunk to improve existing anomaly detection and analysis capabilities; and
  - Develop and deploy custom dashboards and visualizations or modify existing ones.

3.3 Assessing Security through Exercises, Assessments, and Penetration Testing

ISD conducts penetration testing to uncover potential weaknesses, fingerprint behaviors of attackers, and detect potential malicious behavior. This task is not associated with vulnerability testing, or to be staffed by vulnerability testers. It must be staffed with penetration testers who will create new exploits to demonstrate how an attacker could obtain access and compromise the confidentiality, integrity, or availability of USCIS systems. This task includes conducting live security exercises to test the USCIS and other DHS Security Operations Centers (SOC) ability to detect, respond, and recover from a simulated cyber security incident.

The Contractor shall:

- Develop formal penetration testing engagement documentation including the scope, duration, boundaries, targets, risk acceptance documents, and/or others as requested by the Government.
- Execute penetration testing services based on the engagement documentation. As example, this includes, but is not limited to: password strength and quality assessments; SIEM gap analysis, Web Application testing and exploitation, wireless network exploitation, phishing campaigns, data exfiltration, automated network share crawls for PII and other sensitive data, exploitation of lateral movement, and cryptographic strength assessments. As directed, these tests may be performed on internally-developed USCIS applications and general support systems, other DHS applications and general support systems, or cloud services used and accredited by USCIS or other DHS components.
- Coordinate testing with stakeholders of the affected systems, including, but not limited to: system owners, IT project managers, Information System Security Officers, the Security Operations Center, and/or others as directed by the Government.
- Perform custom exploit development for internally-developed USCIS applications and general support systems, other DHS applications and general support systems, or cloud services used and accredited by USCIS or other DHS components.
- Perform detection evasion techniques during penetration testing, including antivirus evasion, log evasion and alteration, encoding of payloads, custom shellcode creation and other techniques popular in the penetration testing community.
- Prepare formal penetration testing results reports, including but not limited to: the findings of the penetration assessment, recommendations for mitigating risk, and lessons learned.
- Design, prepare, and execute live security exercises with USCIS and other DHS Security Operations Centers. These exercises shall assess the effectiveness of preventative controls, the ability of detective controls to detect exercise behavior, and the SOC's ability to detect, respond, and recover from the security incident. Each exercise shall be fully documented to include:

  - An exercise plan that documents the exercise purpose, threat being simulated, controls being assessed, exercise methodology, associated risks, and communications plan;
  - An exercise report that fully documents the exercise including the start and stop times, specific actions taken by the exercise administrators, communications by the SOC and other exercise participants, time to resolution, etc.; and
  - An after action report that documents and analyzes participant actions versus expected actions, whether the participant actions were effective in detecting and responding to the incident, areas that were successful, and specific areas for improvement.
- Communicate with exercise stakeholders to coordinate exercise implementation.

3.4 Application Security Code Review

This task supports the security activities associated with reviewing source code for custom developed USCIS applications or applications used by USCIS. By providing systems and applications support, the Contractor will provide analysis of legacy custom software, web mobile code, database code, and potentially assembly-level issues. The USCIS application inventory includes new and legacy systems with complex data flows. In some cases, legacy code issues must be unraveled to facilitate upgrade and migration to newer systems. Security code reviews will be expected to be operated continuously to support the development pipeline, with ongoing analysis and fine-tuning to reduce false positives. USCIS' goal is to incorporate security code reviews and secure coding practices as early in the software development life cycle as possible.

The Contractor shall:

- Conduct web application and code testing for all systems and applications within the USCIS environment, and open source dependencies, providing analysis and risk assessments for vulnerabilities discovered. The Contractor shall provide highly skilled developers with deep understanding of secure coding concepts and practices, skilled in writing and correcting coding mistakes for source code written in Java, Ruby, C#, Javascript, and other languages.
- Utilize code analysis and fuzzing tools that are furnished or approved by the Government to assess the quality and security of USCIS source code.
- Define secure coding standards and develop secure coding training for current and future developers.
- Conduct code reviews for all code changes for a given application release, providing both a detailed risk analysis of the security posture of the code and technical programming solutions (secure coding standards) to the developers to mitigate insecure code from being implemented.
- Apply the DoD-DHS Software Assurance Forum guidance to USCIS/DHS Systems Lifecycle Process, software development, and engineering principles.
- Provide a monthly report on the overall quality of USCIS source code from a security perspective. This report shall include reports of quality by project and/or development team and shall include trend analysis to identify the number of new defects introduced per release, defects remediated in each release, and trends in the types of defects introduced and remediated.
- Provide devops evaluation, implementation, and operations support for USCIS static and dynamic code analysis tools (currently HPe WebInspect Enterprise, and HPe Fortify). This includes user account and access management, server management, monitoring, patching, version upgrades, and integration with continuous integration/continuous delivery pipelines.

The contractor shall assist the government in performing market research to identify and implement new tools that provide better code analysis or support languages not currently support by USCIS current toolsets.

3.5 Securing the Network

This task supports the security activities associated with evaluating and improving the security of the USCIS network. The Contractor shall:

- Evaluate, deploy, implement, and operate solutions designed to improve the security of the USCIS network including, but not limited to:
  An Intrusion Detection System;
  An Intrusion Prevention System;
  A Network Access Control;
  A Network discovery, mapping, and visualization; and
  Implementation of new solutions for Guest Wireless networks
- Evaluate current and future network designs to ensure that security is incorporated as an integral consideration in these designs.
- Audit firmware versions and configuration settings for all USCIS network devices to eliminate vulnerabilities and ensure USCIS network devices are deployed in accordance with vendor recommendations, industry best-practices, DoD STIGs, and DHS configuration guidance.
- Review existing configuration settings to identify potential security vulnerabilities and propose setting or architectural changes to address these vulnerabilities.
- Work collaboratively with other contractor teams to improve the use of automated configuration management capabilities to enforce security-relevant configuration settings.
- Perform securing hardening and rule creation for new firewalls, switches, routers and other network equipment. This includes reviewing and re-evaluating existing configuration settings and rules to verify USCIS' security posture and eliminate unnecessary risk.

3.6 Maintaining Security Hygiene

Good security hygiene is one of the foundations of a quality security program. This includes scanning USCIS IT assets to verify they do not have known vulnerabilities, are configured in accordance with USICS standards and industry best practices, and are running current, patched versions of COTS and open oksource applications.

The Contractor shall:

- Create secure configuration settings for commonly used software applications and operating systems. As directed by the program manager, the contractor shall develop secure configuration settings for Red Hat Enterprise Linux 7 (or most current version), CentOS 7 (or most current version), Ubuntu 16.04 server (or most current version), CoreOS (current version), Alpine Linux (current version), and Microsoft 2016 Server (all editions, current version). As part of this effort, the Contractor shall develop hardening scripts to implement these settings using Ansible, Chef, Powershell or other technologies to implement these settings. All scripts and configuration settings shall be documented and maintained in USCIS' GIT.
- Support vulnerability and compliance scanning of the USCIS computer environment. This scanning includes scanning for vulnerabilities and compliance with defined security settings at the operating system, web, application, and database layers.

- Collaborate with USCIS system owners, IT project managers, and other devops engineers to identify and resolve the causes of delayed patching.
- Develop communication materials to document the security status of each application and progress in addressing vulnerabilities and configuration misconfigurations.
- Implement and operate USCIS security tools. The contractor shall be responsible for engineering the deployment, deploying, testing, maintaining, patching and operating the tools. The contractor must provide experienced systems administrators, with experience using configuration management tools (e.g. Ansible, Chef, PowerShell) to manage the system. USCIS anticipates it will deploy additional security tools to meet critical security needs during the period of performance of this contract. As USCIS deploys additional security tools the vendor shall deploy, maintain, and support these tools. The current security tools for which the vendor must provide support are:

  Splunk
  Exabeam Threat Hunter
  Beyond Trust Retina
  Forescout CounterACT
  CyberArk
  FireEye HX
  Tenable SecurityCenter
  McAfee Endpoint Security Products (VirusScan, Digital Loss Prevention, Application Control, Host Intrusion Protection, Configuration Control, and Deep Command)
  Trustwave DbProtect
  HPe WebInspect
  HPe Fortify
  CA Xceedium
  NetWitness
  Invincea
- For McAfee:

  Complete the deployment of McAfee Application Control in application whitelisting mode; develop custom application policies for USCIS software; coordinate with other USCIS teams to integrate Application Control into USCIS software asset and software management processes.
  Complete the deployment of McAfee HIPS to USCIS workstations and servers; develop custom HIPS rules and work with DevOps teams to implement these rules.
  Deploy DeepCommand to enable after-hours patching and software installations
  Implement new DLP rules to prevent USCIS information from being exfiltrated
- Complete development of and provide ongoing support for Asset Manager, a USCIS developed asset management tool used to track computing assets, store metadata regarding these assets, assign them to FISMA systems, and request security scans of these assets.

3.7 Implementing the Continuous Diagnostics and Monitoring Program

The DHS Continuous Diagnostic and Monitoring Program will implement a baseline set of standardized security capabilities across the Federal government. The Contractor shall provide project/program management support to help the government coordinate the activities of multiple organizations to implement the CDM program within USCIS.

The Contractor shall:

- Manage the program schedule for the implementation of CDM within USCIS, and provide regular status reports on the implementation progress, risks, and issues of each project to the USCIS CDM program manager.
- Develop and review program documentation and ensure the implementation of each CDM project is documented to USCIS standards.
- Develop and submit change requests, infrastructure service requests, and other change management documentation to further the implementation of CDM-related projects.
- Collaborate with other USCIS engineering, development, and security teams to brief and inform them of the work that needs to be performed in order to complete the implementation of CDM-related projects. The Contractor is responsible for providing technical guidance to other USCIS teams, coordinating between USCIS teams and the CDM PMO, monitoring the priority of the work (e.g. whetherwork has been assigned its implementation status, and if there are any risks, or barriers to completing the implementation.)

The Contractor is responsible for collaborating with other teams and coordinating the next steps ofwork that needs to be performed and providing technical guidance on specific tasks. The contractor shall not task USCIS employees or other contractor teams. It is solely the Government's responsibility to prioritize, order, and assign this work.

3.8 Supporting Enterprise Security Engineering

This task is primarily intended to support the security activities required to support other agile teams to incorporate security into the development of new solutions and recommend security best practices associated with the development of new enterprise applications in an Agile/DevOps environment.

The Contractor shall:

- Perform hands-on technical security risk assessments to identify flaws, threats and risks in emerging IT projects at USCIS, and develop technical in-depth engineering solutions to address and mitigate these risks.
- Lead the DevOps team with the design, implementation and management of security solutions which leverage automation, near real-time security feedback, repeatable processes, continuous integration and continuous deployment methodologies, to achieve a rugged DevOps environment with a zero security defect mentality.
- Provide technical security solutions and control implementation recommendations to the Agile Development teams based on industry best practice and Federal requirements.
- Implement automated, scripted security controls testing for DevOps projects, to streamline technical controls testing, and reduce testing time to minutes rather than days or weeks.
- Provide security testing services to validate how well a system meets predefined security requirements.
- Provide security engineering and test services with specific regard to the mitigation of unauthorized access, leakage of data, manipulation of data, or willful damage.
- Provide security testing support to establish an application's security baseline and identify a level of security risk prior to production implementation.
- Attend Agile Scrum Methodology Sprints and Increments and provide solutions and guidance to developer security questions or issues.
- Identify risks associated with implementing given user stories into a product.

- Create security controls through “security user stories” based on NIST SP800 guidance, DHS policy, USCIS policy, and industry best practice (i.e. OWASP) to mitigate information security risk. Security user stories shall be organized, categorized, prioritized and updated to allow efficient and effective re-use of stories across the enterprise, and documented in a format which is easy to share and explain to stakeholders. Security user stories shall include testable acceptance criteria and clear definitions for completion and closure.
- Design security tests to assess the controls and overall security of the implemented user stories for each product.

3.9 Developing Enterprise Security Solutions

This task is primarily intended to support the security activities associated with the evaluation, implementation and continued operation of new security technologies into the USCIS enterprise.

The Contractor shall:

- At the discretion of the Federal task lead, architect, implement, deploy and operate a wide range of enterprise security solutions to address a broad set of security needs including, but not limited to: Vulnerability Management, Configuration Management, Network Access Controls, Malware Defenses, Application Software Security, Security Code Review, Software Asset Management, Hardware Asset Management, Vulnerability Remediation, Security Event and Log Management, Incident Response, Penetration Testing, Wireless Access Control, Least Privilege, Network Monitoring, Boundary Defense, Security Assessment, Account Monitoring and Control, Data Protection, Insider Threat, Continuous Monitoring, and/or others as requested by the Government.
- Automate and streamline repetitive IT security processes, and the handling of vast amounts of security data, at the discretion of the Federal task lead, using programming and the Security Event Management framework to consolidate security information and reporting.
- Create actionable intelligence through triggers, filters, and signatures that pinpoint threats contained within the Security Event Management system for the Security Operations Center to investigate from new and existing continuous monitoring security products, such as, but not limited to: Beyond Retina, Forescout, CyberArk, Tenable SecurityCenter, McAfee EPO, DbProtect, Splunk, CISCO ISE, IDS, IOS and Microsoft SCCM, WSUS, Xceedium, NetWitness, HP WebInspect and Fortify, etc.
- Attend all meetings, design reviews, engineering conference calls, system readiness reviews, and participate in Integrated Planning Teams (IPTs) and/or Scrum Sprints/Increments to monitor security requirement execution throughout the USCIS/DHS Systems Lifecycle process and deliver minutes, and any ad-hoc project reporting requested by the Government.
- Implement, support, and write filters, plugins, access control lists, and monitoring rules for new and existing continuous monitoring security products, such as, but not limited to: Tenable SecurityCenter, McAfee EPO, DbProtect, Splunk, ArcSight, CISCO ISE, IDS, IOS, and Microsoft SCCM, WSUS, Xceedium, NetWitness, HP WebInspect and Fortify, etc.
- Write system lifecycle documentation for security products or security-relevant system components. This includes, but is not limited to: Project architecture diagrams, project plans and timelines, Concepts of Operations, Standard Operating Procedures, use cases, user stories, change management documents, system lifecycle documentation, technical implementation strategies, and product specific configurations that align with USCIS policy and procedure, DHS

policy and procedure, DHS continuous monitoring requirements and annual metrics, and NIST Special Publication 800 Guidance.

- Evaluate best-of-breed products and standards, consistent with Federal security guidance.
- Perform product/standards comparisons based upon research, independent lab test result reports, intelligence agency recommendations, and other resources authoritative, mandatory, or compelling to a U.S. Federal agency.
- Identify and evaluate information security threat models and methodologies. Manage the implementation and maintenance of the selected methodologies by applying the threat model to support ongoing, proactive protection of the USCIS enterprise environment, and to facilitate an efficient response to security incidents. Develop standards, templates and automated mechanisms to support threat modeling and analysis of individual USCIS information systems and information. Provide recurring inputs, triggers and reporting into the USCIS Security Information Event Management tool and Ongoing Authorization processes.
- At Government direction, schedule and attend conference calls, meetings, demonstrations, conferences, trade shows, and other events with third-party equipment, software, and service vendors for the purposes of market research. Provide expert opinion to Federal manager, but will not make product/standards selections on behalf of the Government. Product/standards selection will only be performed by the Government.
- Support the design and deployment of information security solutions at all layers of the OSI model, physical layer to application layer, to facilitate a comprehensive defense-in-depth strategy and intrusion defense chain methodology.
- Be responsible for the technical configuration and installation of products into a pilot/evaluation location established via the USCIS Change Request (CR) process.
- Generate procedures necessary to operate and maintain products under pilot/evaluation.
- Generate USCIS/DHS Systems Lifecycle Process documentation necessary to obtain engineering approval for products under pilot/evaluation.
- Generate the Enterprise Architecture (EA) documentation necessary to obtain Technical Reference Model (TRM) approval for products under pilot/evaluation.
- Schedule and attend meetings, file USCIS forms, tickets, and change requests necessary to facilitate successful deployment of security products/projects.
- Generate and present formal reports and presentations that explain and defend the recommended product selections in meetings designated by the Government POC requesting the evaluation.

3.10 Securing the Cloud

USCIS is making major investements in moving to Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) cloud vendors for the majority of its computing needs. As USCIS moves to the cloud, it requires skilled resources that understand how security in the cloud is similar to that of on-prem data centers and the key differences that require different controls and different approaches.

The Contractor shall:

- Develop best practice security guidance for developing and deploying applications in an Amazon Web Services or other cloud environment.

- Develop scripts, wikis, training briefings, webinars, and other documentation to implement this guidance as we as to make other USCIS employees and contractors aware of new security offerings provided in the cloud by USCIS ISD or the cloud vendor.
- Develop functions for AWS Lambda or other Function as a Service offerings that test and maintain key cloud security controls (e.g. enforcing restrictions on Internet Gateways and preventing S3 buckets from being made public)
- Develop CloudFormation templates for creating new accounts and new VPCs with USCIS security requirements enabled by default (e.g. CloudTrail, CloudWatch)
- Develop scripts, dashboards, and other reports that provide automated reporting and notification of current USCIS cloud security settings that are at variance from USCIS security requirements.
- Provide cloud security expertise to other USCIS organizations and serve as the USCIS expert on how to deploy applications securely to AWS and other cloud environments.

4 Teams and Personnel Qualifications

4.1 Key personnel

The following personnel are deemed key personnel:

- (1) CSDS Program Manager (4.2)
- (1) Sr. Splunk Engineer Level III (4.3)
- (1) Sr. Penetration Tester Level III (4.4)
- (1) Network Engineer Level III (4.5)
- (1) Sr. Security Tools Engineer (Security Engineer III) (4.7)

4.2 Program Management and Project Planning

To provide effective project and program management, the Contractor shall provide a full time program manager to oversee all tasks on the contract. The program manager shall have the following qualifications:

- Ten (10) or more years of experience in project and program management including:
  - At least five (5) years of experience managing IT projects and programs.
- PMI Project Management Professional (PMP) certification.

4.3 Detecting Security Incidents

Shall be staffed with one (1) Senior Splunk Engineer and one (1) Mid Splunk Engineer.

The Senior Splunk Engineer shall have the following qualifications:

- Eight (8) or more years of experience in IT security, administration and/or operations including:
  - At least four (4) years of specialized experience deploying and operating large, enterprise-wide Splunk clusters;
  - At least three (3) years experience leading the deployment and operations of a large, complex, multi-datacenter Splunk cluster consisting of index clusters at multiple data centers and multiple search head clusters;
  - At least three (3) years experience creating complex security and operations dashboards and alerts for use by multiple stakeholders within the organization; and

  - At least at least two (2) years prior experience deploying or operating Splunk Enteprise Security (ES) and/or Splunk Analytics for Hadoop.
- These positions must be staffed in Washington, DC.

The Mid-level Splunk Engineer shall have the following qualifications:

- Five (5) or more years of experience in IT systems administration and two (2) years of specialized experience in implementing enterprise security products and solutions including:
  - At least two (2) years of Linux systems administration experience; and
  - At least two (2) years prior experience operating a mid-size Splunk cluster or one years experience and Splunk certification.
- This position must be staffed in Washington, DC.

4.4 Assessing Security through Exercises, Assessments, and Penetration Testing

Shall be staffed with two (2) Senior Penetration Testers and one (1) mid-level Penetration Tester.

The Senior Penetration testers must have the following qualifications:

- Eight (8) or more years of experience in IT security including:
  - At least five (5) years specialized experience in penetration testing.
- Demonstrated experience creating novel, reusable, exploits for disclosed and undisclosed vulnerabilities. This experience may also be demonstrated by having one of the following active certifications: Exploit Researcher and Advanced Penetration Tester (GXPN), Offensive Security Certified Expert (OSCE), or Offensive Security Certified Professional (OSCP), Offensive Security Exploitation Expert (OSEE).
- Proficiency in at least one (1) of the following frameworks: Metasploit, Core Impact, Immunity Canvas.
- These positions must be staffed in Washington, DC.

The mid-level Penetration Tester shall have the following qualifications:

- Three (3) or more years specialized experience in penetration testing. Experience responding to Advanced Persistent Threat (APT) type incidents for large enterprises as a member of an incident response team may be substituted for the specialized experience.
- Demonstrated experience creating novel, reusable, exploits for disclosed and undisclosed vulnerabilities. This experience may also be demonstrated by having one of the following active certifications: Exploit Researcher and Advanced Penetration Tester (GXPN), Offensive Security Certified Expert (OSCE), or Offensive Security Certified Professional (OSCP), Offensive Security Exploitation Expert (OSEE) or another comparable certification or other experience which demonstrates an understanding of the concepts covered by these certifications which must be approved in advance by the Government Program Manager on a case-by-case basis. In lieu of certifications, evidence of one or more years experience responding to Advanced Persistent Threat (APT) type incidents for large enterprises is acceptable.
- Expertise creating novel, reusable, exploits for disclosed and undisclosed vulnerabilities or demonstrated expertise using a scripting language such as PowerShell, Python, Ruby, or Perl for penetration testing or incident response.
- Demonstrated experience utilizing at least one (1) of the following frameworks: Metasploit, Core Impact, Immunity Canvas.
- These positions must be staffed in Washington, DC.

4.5 Developing Secure Code

Shall be staffed with two (2) Sr. Security Code Reviewers with the following qualifications:

- Seven (7) or more years of experience in performing software development, and three (3) years of specialized experience performing security code reviews including
  - At least 2 years experience utilizing HPe Fortify or other static and dynamic code scanning tools to perform security assessments.
- A Bachelor's degree in Computer Science, Information Management or Engineering. Any other comparable degree or experience must be approved in advance by the Government.
- One or more of the following active certifications: EC-Council Certified Secure Programmer, Certified Secure Software Lifecycle Professional (CSSLP), SANS Global Information Assurance Certification (GIAC) Secure Software Programmer (.NET or JAVA), HP ATP – Fortify Security V1, or another comparable certification, or other experience which demonstrates an understanding of the concepts covered by these certifications which must be approved in advance by the Government Program Manager on a case-by-case basis.
- Proficiency in analyzing and testing web applications developed in at a minimum of two (2) of the following languages listed below, and in combination, the team must have a proficiency in all of the following languages listed below:
  - Java, JavaScript, Ruby, C#. It is expected that this list of programing languages will evolve and change over time, and that the Contractor will provide expertise in newly introduced languages. New languages if used shall be added to the SOW via modification.
- These positions must be staffed in Washington, DC.

4.6 Securing the Network

Shall be staffed with two (2) Network Engineer Level III and one (1) Network Engineer Level II.

Each Network Engineer Level III shall have the following qualifications:

- Ten (10) or more years of experience in network engineering and operations and three (3) years specialized experience deploying security products (Firewalls, IDS/IPS devices, Lancope, SourceFire IDS, Cisco ISE, ForeScout CounterACT, etc.).
- At least one (1) of the following active certifications: Cisco Certified Internetwork Expert (CCIE) Security, CCIE Wireless, CCIE Data Center, CCIE Routing & Switching, Cisco Certified Network Professional Security (CCNP Security), or other comparable certification or experience, which must be approved in advance by the Government.
- Proficiency in configuring, securing, and creating custom rule sets for: Cisco Nexus, Flexpod, IOS, Identity Services Engine (ISE), Cisco Sourcefire and any other additional networking technologies introduced by the Government during the duration of the contract.
- Prior experience utilizing Cisco Prime, Orion Solarwinds or another configuration management tool to create enforceable configuration templates.
- Contractors shall be located at the government's facility in Williston, VT.

Each Network Engineer Level II shall have the following qualifications:

- Five (5) or more years experience in network engineering and operations including at least two (2) years of specialized experience deploying security products (Firewalls, IDS/IPS devices, Lancope, SourceFire IDS, Cisco ISE, ForeScout CounterACT, etc.).
- At least one (1) of the following active certifications: Cisco CCDP or any Cisco CCNP certification, or other comparable certification or experience, which must be approved in advance by the Government.

- Proficiency in configuring, securing, and creating custom rule sets for: Cisco Nexus, Flexpod, IOS, Identity Services Engine (ISE), Cisco Sourcefire and any other additional networking technologies introduced by the Government during the duration of the contract.
- Prior experience utilizing Cisco Prime, Orion Solarwinds or another configuration management tool to create enforceable configuration templates.
- This position must be staffed at the Government's facility in Williston, VT.

4.7 Maintaining Security Hygiene, Supporting Enterprise Security Engineering, and Developing Enterprise Security Solutions

Personnel supporting these tasks are anticipated to divide their time between these tasks according to support needs. These tasks shall be staffed as follows:

- 1 Sr. Linux Systems Security Engineer
- 1 Sr. Windows System Security Engineering
- 2 Sr. Security Tools Engineer (Security Engineer III)
- 1 Mid Security Tools Engineer (Security Engineer II)
- 1 Sr. Application Development Engineer
- 1 Jr. Security Tools Engineer (Security Engineer II)

The Senior Linux Systems Security Engineer shall have the following qualifications:

- Seven (7) or more years experience, installing, configuring, operating, and patching Linux servers.
- Advanced knowledge of one or more of the following configuration management tools: Ansible, Chef, Puppet, SaltStack.
- Understanding of New Relic or Nagios monitoring
- Two (2) or more years experience deploying applications to Amazon Web Services.
- This position must be staffed in at the Government's facility in Williston, VT.

The Senior Windows System Security Engineer shall have the following qualifications:

- Ten (10) or more years experience administering large, complex Windows applications and/or as a Active Directory Domain Administrator.
- Expert knowledge of PowerShell and Group Policy
- This position must be staffed in at the Government's facility in Williston, VT.

The Senior Security Tools Engineers shall have the following qualifications:

- Eight (8) or more years of experience in IT security, including 5 years of specialized experience in implementing enterprise security products and solutions.
- A Bachelor's or Master's degree in Computer Science, Information Management or Engineering. Any other comparable degree or experience must be approved in advance by the Government.
- At least one team member shall have prior experience leading the deployment and operation of vulnerability assessment tools, such as Tenable Security Center or Beyond Trust Retina to a large enterprise.
- At least one (1) team member shall have prior experience leading the deployment and operations of a large, complex, McAfee Endpoint security installation at a large enterprise. This individual must have experience deploying and operating at least three (3) of the following:
  McAfee Host Instrusion Prevention
  McAfee Digital Loss Prevention

McAfee Application Control
McAfee Deep Command
McAfee Drive Encryption

- One (1) position mustll be staffed in Williston, VT area and one (1) must be staffed in Washington, DC area. Either position may be staffed at other locations in the United States with approval by the Government.

The Mid Security Tools Engineer shall have the following qualifications:

- Five (5) or more years of experience in IT security, including three (3) years of specialized experience in implementing enterprise security products and solutions.
- A Bachelor's or Master's degree in Computer Science, Information Management or Engineering. Any other comparable degree or experience must be approved in advance by the Government.
- This position must be staffed in the Washington, DC area.

The Sr. Application Development Engineer shall have the following qualification:

- Five (5) or more years experience developing applications using the Ruby on Rails Framework.
- A Bachelor's or Master's degree in Computer Science, Information Management or Engineering. Any comparable degree or experience must be approved in advance by the Government.
- This position may be staffed anywhere in the United States.

The Jr. Security Tools Engineer shall have the following qualifications:

- A Bachelor's or Master's degree in Computer Science, Information Management or Engineering.
- This position must be staffed at the Government's facility in Williston, VT.

4.8 Implementing the Continuous Diagnostics and Monitoring Program

Shall be staffed with one (1) Project Manager II with the following qualifications:

- Five (5) or more years experience managing IT security projects
- Active Project Management Professional or higher certification from Project Management Insitute; or other comparable certification or experience, which must be approved in advance by the Government.
- This position must be staffed at the Contractor's location in Washington DC.

4.9 Securing the Cloud

Shall be staffed with one (1) Cloud Security Engineer Level III with the following qualifications:

- Seven (7) or more years experience engineering, developing and deploying IT systems. At least three (3) years experience as a Senior Engineer deploying, operating, or providing IT security engineering for systems deployed in AWS.
- At least one (1) year experience using Python, Ruby, or Java to automate operations or security functions using the AWS SDK and AWS Lambda.
- At least two (2) years experience using Chef, Ansible, Terraform, CloudFormation or other tools to automate infrastructure deployments in AWS.
- Active AWS Solutions Architect or AWS Certified DevOps Engineer certification
- This position may be staffed anywhere in the United States.

5 Task Order Administration Data

5.1 Place of Performance

The principal place of performance shall be at the contractor provided work site. The contractor facility shall be in close proximity to the USCIS facilities at 131 M Street N.E., Washington, DC and 111 Massachusetts Ave N.W., Washington D.C.. However, the Government may elect to have Contractor personnel perform work onsite at USCIS facilities for certain task areas. As designated in section four, key personnel shall work on-site at USCIS' locations in Williston, VT and Washington, DC.

All contractor personnel shall be capable of teleworking from a home-office location via secure VPN over a reliable Internet connection provided by the contactor with a Laptop provided by the Government (GFE).

Meetings will typically be held at USCIS offices in the Washington, D.C. Metropolitan Area, including, but not limited to 131 M Street N.E., 111 Massachusetts Ave N.W., and 20 Massachusetts Avenue N.W., Washington DC. Meetings may also occur at the contractor's work site, particularly when close collaboration between stakeholders and the team is needed. The Contractor shall provide meeting space such as a team room, to accommodate up to five Government representatives. The contractor shall also provide meeting space for periodic hosting of meetings with both USCIS federal and contractor personnel.

5.2 Hours of Operation

The contractor shall provide support from 8 AM to 5 PM. This time period includes a 1 hour unpaid lunch period. Contractor's personnel shall be available during core working hours, which is defined as 9 AM to 3 PM Eastern Time, Monday thru Friday, excluding holidays. The contractor will be required to provide on-call after-hours support for outages of supported security tools that cause a work stoppage for a significant number of USCIS users or cause an outage for a major USCIS application. After-hours support is expected to be infrequent, typically only occurring in conjunction with updates to USCIS security tools being made by the contractor. The following contractor personnel must be available for on-call after hours support when needed:

- One of the Network security engineers identified in section 4.6
- One of the Security engineers identified in section 4.7

The contractor will also be required to provide after-hours support for deployments, system maintenance, changes, security emergencies, or other operational requirements that cannot be performed during normal working hours. The contractor may request hours for extended work week if the USCIS Program Manager authorizes in advance to support such extigent circumstances impacting operations.

5.3 Government Furnished Property (GFP)

Only GFP computing devices will be issued and used in performing work on this contract. No personal or company owned storage devices, (thumb drives, DVDs, or CDs) will be used with the GFP.

The Contractor shall:

- Ensure that all USCIS, DHS, and Government-furnished data is transmitted, processed, protected, and stored on GFP.
- Use only GFP hardware, software, devices, or other equipment and ensure the full inventory allotted to the Contractor is available and accountable at all times.

For the purposes of this section, DHS and/or USCIS Workplace as a Service is considered GFP and is authorized to be accessed using contractor or personally-owned equipment.

The following GFP is anticipated to be issued to support the performance of this contract:

Quantity	Item	Estimated Value
20	Laptop computer	$2,500
9	Apple MacBook	$4,000

5.4 Travel

Travel within the local commuting area will not be reimbursed. For the purpose of this Task Order the local commuting area is defined as a fifty (50) mile radius from the primary place of performance. For contractor personnel who work on-site in USCIS offices, the local commuting area is defined as a fifty (50) mile radius from the USCIS site. Home to work travel is not reimbursable.

Travel may be required at the following USCIS Office locations (this list is not exhaustive): California Service Center, Vermont Service Center, Nebraska Service Center, Texas Service Center, New York Field Office, and National Records Center. All travel shall be at the Government's direction and shall be pre-approved by the COR in writing before execution. Travel shall be in accordance with applicable federal travel regulations.

Please reference Paragraph H.6.1 of the EAGLE II Contract for further information regarding travel.

5.5 Transition

Contract transition is a challenging effort that encompasses all activities needed to transfer operations from one contract to another, set up the effort, and on-board employees. Contractors are expected to implement transition and application cutover activities in such a manner as to cause no disruption in services. The incoming contractor will have access to the outgoing contractor upon task order award. The main activities for transition include the task order award meeting, on-boarding of personnel, development and delivery of transition reports, and transfer of work for 90 days from the task order award. At the culmination of this activity, contractor personnel should be ready to work activities other than transition.

A comprehensive transition plan will be provided by the government. The incoming contractor shall review, provide feedback or concerns, and ultimately come to an agreement and sign the transition plan provided by the government. There will be approximately 30 days from task order award for the contractor to start on-boarding employees and receive security clearances for a partial notice to proceed to be issued. After the partial notice to proceed is issued there will be approximately 60-days for a “transition-in” period to transfer the responsibilities from the incumbent contractor to the new contractor.

At the completion of performance of this task order, the contractor shall fully support the transition of the work that is turned over to another entity, either government or a successor in accordance with FAR 52.237-3. The contractor shall assist with transition planning and shall comply with the transition milestones and schedule. To ensure the necessary continuity of services and to maintain the required level of support, USCIS may retain services of the incumbent contractor for some or all of the transition period, as required. The contractor shall be responsible for the transition of all technical activities identified in this task order

6 Deliverables

The primary deliverables of this task order are deployable information security solutions, and documentation and processes supporting the security authorization of USCIS systems. The Contractor shall deliver these items throughout the period of performance. All deliverables shall be provided to the Government with unlimited rights as per FAR 52.227-17.

The Contractor shall submit electronic copies of document deliverables that are indicated in the table below to the CO and COR (and other cc’s as may be specified by the CO and/or COR) via email in the format specified. All document deliverables shall be made by close of business on the business the delivery is required, Monday through Friday, unless stated otherwise.

6.1 Deliverables Schedule

Section	Item	Frequency of Delivery	Acceptable Formats
6.3	Weekly Status Report	Each Friday	MS Word or MS PowerPoint
6.4	Monthly Status Report	Monthly, the first Friday of the month.	MS Word or MS PowerPoint
3.2	Splunk System Maintenance and Configuration Scripts	Continuous delivery in GIT	As directed by the Government Program Manager and delivered to USCIS GitHub Enterprise
3.3	Penetration Test Rules of Engagement	At least 10 days prior to initiation of a penetration test (This may be waived by Government Program Manager in case of expedited tests)	MS Word
3.3	Penetration Test Plan	10 days prior to initiation of a penetration test (This may be waived by Government Program Manager in case of expedited tests)	MS Word
3.3	Penetration Test Detailed Report	Within 5 days of the completion of a penetration test	MS Word
3.3	Penetration Test Executive Summary Report	Within 5 days of the completion of a penetration test.	MS PowerPoint

Section	Item	Frequency of Delivery	Acceptable Formats
3.3	Security Exercise Plan	5 days prior to initiation of a security exercise	MS Word
3.3	Security Exercise Report	Within 5 days of the completion of a security exercise	MS Powerpoint
3.4	Monthly Code Quality Status Report	Monthly, the first Friday of the month.	MS Powerpoint
3.4	USCIS Secure Coding Standards	Initial delivery within 180 days of receiving a notice to proceed. Monthly updates as directed by the USCIS Program Manager.	MS Word
3.4	Secure Coding Developer Training	Initial delivery within 90 days of receiving a notice to proceed. Monthly updates as directed by the USCIS Program Manager	MS Word
3.6	Bi-weekly system vulnerability report	First and third Fridays of the month	MS Powerpoint or Splunk Dashboard
3.6	Bi-weekly system configuration report	Second and fourth Fridays of the month	MS Powerpoint or Splunk Dashboard
3.8	Weekly CDM Status Report	Each Friday	MS Word or MS PowerPoint
3.8	CDM Schedule	As directed by the Government Program Manager	MS Project or Leankit
3.8	CDM Communications Briefings	As directed by the Government Program Manager	MS PowerPoint or as mutually agreed upon
3.9	Technical security risk assessments	As directed by the Government Program Manager	MS Word or as mutually agreed upon
3.9	System Lifecycle Documentation	As directed by the Government Program Manager	MS Word or as mutually agreed upon
3.9	Product Evaluation Memorandum	As directed by the Government Program Manager	MS Word or as mutually agreed upon
HSAR	Security Plan	30 day ARO and after major changes	MS Word
3.1	Separation Notification	By close of business of the separation date.	MS Word or as mutually agreed upon

6.2 Project Management Plan

The Contractor shall prepare a Project Management Plan that facilitates its implementation of continuous delivery precepts describing the technical approach, organizational resources, and management controls they will employ to meet the cost, performance, and schedule requirements throughout SOW execution.

6.3 Weekly Status Report (WSR)

The Contractor shall submit a WSR in accordance with the delivery schedule. The WSR shall include:

- Summary of weekly project and program activities
- List of tasks assigned by task area and team

- List of accomplishments and completed tasks and deliverables by task area and team
- Outstanding project and task concerns
- Activities planned for the upcoming week by task area and team
- Kanban board with status of projects by task area and team
- Staffing Performance Measure: List of all required positions mapped to contractor names with work status (active or vacant) and labor category by task area and team
- Progress on staffing plan to include status on entry on duty (EOD) and training requirements

6.4 Monthly Status Report (MSR)

The Contractor shall submit a MSR in accordance with the delivery schedule. The MSR shall include:

- An overview of work completed, in progress, and planned for each task area and team
- Identification of problem areas with recommended remedial actions
- Performance measurement input (by task area and team)

  Productivity Performance Measure: A summary of work activities planned and committed by task area and team for each two week work cycle (sprint) during the month. A summary of work activities completed and delivered (from the activities planned and committed above) by task area and team for each two week work cycle (sprint) during the month. Calculation of Velocity by task area and team (sum of two week work cycle for the month): Total Completed/Delivered Work Activities divided by Total Planned/Committed Work Activities.

  Quality and Standards Adherence Performance Measure: A summary of documents and deliverables submitted to the Government by task area and team during the month. A summary of documents and deliverables (corresponding to the list above) submitted to the Government which required more than two Government reviews to achieve Government acceptance.

6.5 Inspection and Acceptance

Inspection and acceptance of deliverables will use the following procedures:

- The government will provide written acceptance, comments, and/or change requests, if any, within ten (10) calendar days of receipt of task order deliverables.
- If government acceptance, comments, and/or change requests are not provided to the contractor within 15 calendar days after delivery of a deliverable, the contractor shall assume government acceptance.
- Upon receipt of the government comments, the contractor shall, within three (3) business days, rectify the situation and re-submit the contract deliverable(s).

7 References

The Contractor shall be subject to all current and future versions of DHS Sensitive Systems Policy Directive 4300A, DHS National Security Systems Policy 4300B, the annual DHS Information Security Performance Plan, National Institute of Standards and Technology (NIST) Special Publication (SP) 800 Series, Federal Information Processing Standards (FIPS) and all associated USCIS policies including all associated attachments, concepts of operation (CONOPS), processes and standard operating procedures. Documents which are not publically available will be provided to the selectee upon contract award.

U.S. Citizenship and Immigration Services
Office of Security and Integrity – Personnel Security Division

SECURITY REQUIREMENTS

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 classified National Security Information (herein known as classified information). Classified information is Government information which requires protection in accordance with Executive Order 13526, Classified National Security Information, and supplementing directives.

The Contractor shall abide by the requirements set forth in the DD Form 254, Contract Security Classification Specification, included in the contract, and the National Industrial Security Program Operating Manual (NISPOM) for the protection of classified information at its cleared facility, if applicable, as directed by the Defense Security Service.

Any firm or business under contract with the Department of Homeland Security (DHS), which requires access to classified information, will require a facility security clearance commensurate with the level of access required. Firms that do not possess a facility clearance, or the requisite level of facility clearance, will be sponsored for a Department of Defense facility clearance.

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 and/or classified information, shall undergo a position sensitivity analysis based on the duties each individual will perform on the contract as outlined in the Position Designation Determination (PDD) for Contractor Personnel. 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.

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. Position Designation Determination for Contract Personnel Form

5. Foreign National Relatives or Associates Statement

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

7. ER-856, “Contract Employee Code Sheet”

EMPLOYMENT ELIGIBILITY

Be advised that unless an applicant requiring access to sensitive but unclassified information and/or classified 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.

VISIT AUTHORIZATION LETTER (VAL)

The Contractor is required to submit a VAL for those individuals who require access to classified information during performance on this contract and who have an active Personnel Security Clearance (PCL). The letter will be valid for a period not to exceed one year. If the requirement to access classified information no longer exists, or if access eligibility changes, OSI will be notified immediately. The VAL must be submitted to OSI PSD in accordance with, and contain information as required by, Chapter 6 of the NISPOM.

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, 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 duty for new contractors, and annually thereafter)
- **USCIS Integrity Training** (Annually)
- **DHS Continuity of Operations Awareness Training** (one-time training for contractors identified as providing an essential service)
- **USCIS Office Safety Training** (one-time training for contractors working within USCIS facilities; contractor companies may substitute their own training)
- **USCIS Fire Prevention and Safety Training** (one-time training for contractors working within USCIS facilities; contractor companies may substitute their own training)

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 out so 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 Facility 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.

Contractor employees who become eligible for access to classified National Security Information shall participate in annual USCIS NSI refresher briefings. Briefings be coordinated through the COR, PSD and the OSI Administrative Security Division.

In the event classified information is inadvertently received by a contractor who does not hold an active security clearance at the Secret level, a Government employee or Contractor with the appropriate security clearance equal to or higher than the classified information received, will take possession of the material and shall safeguard and store the information in accordance with standards set forth in the NISPOM. The inadvertent disclosure will be immediately reported to their supervisor and then to the designated OSI Local Security Officer or OSI Field Security Manager for action as appropriate.

In the event classified information is inadvertently received by a contractor who does not hold an active security clearance at the Secret level, a Government employee or Contractor with the appropriate security clearance equal to or higher than the classified information received, will take possession of the material and shall safeguard and store the information in accordance with standards set forth in the NISPOM. The inadvertent disclosure will be immediately reported to their supervisor and then to the designated OSI Local Security Officer or OSI Field Security Manager for action as appropriate.

Subpart 4.4—Safeguarding Classified Information Within Industry

4.402 General.

(a) Executive Order 12829, January 6, 1993 (58 FR 3479, January 8, 1993), entitled "National Industrial Security Program" (NISP), establishes a program to safeguard Federal Government classified information that is released to contractors, licensees, and grantees of the United States Government. Executive Order 12829 amends Executive Order 10865, February 20, 1960 (25 FR 1583, February 25, 1960), entitled "Safeguarding Classified Information Within Industry," as amended by Executive Order 10909, January 17, 1961 (26 FR 508, January 20, 1961).

(b) The National Industrial Security Program Operating Manual (NISPOM) incorporates the requirements of these Executive orders. The Secretary of Defense, in consultation with all affected agencies and with the concurrence of the Secretary of Energy, the Chairman of the Nuclear Regulatory Commission, and the Director of Central Intelligence, is responsible for issuance and maintenance of this Manual. The following DoD publications implement the program:

(1) National Industrial Security Program Operating Manual (NISPOM) (DoD 5220.22-M).

(2) Industrial Security Regulation (ISR) (DoD 5220.22-R).

(c) Procedures for the protection of information relating to foreign classified contracts awarded to U.S. industry, and instructions for the protection of U.S. information relating to classified contracts awarded to foreign firms, are prescribed in Chapter 10 of the NISPOM.

(d) Part 27—Patents, Data, and Copyrights, contains policy and procedures for safeguarding classified information in patent applications and patents.

4.403 Responsibilities of Contracting Officers.

(a) *Presolicitation phase*. Contracting officers shall review all proposed solicitations to determine whether access to classified information may be required by offerors, or by a contractor during contract performance.

(1) If access to classified information of another agency may be required, the contracting officer shall—

(i) Determine if the agency is covered by the NISP; and

(ii) Follow that agency's procedures for determining the security clearances of firms to be solicited.

(2) If the classified information required is from the contracting officer's agency, the contracting officer shall follow agency procedures.

(b) *Solicitation phase*. Contracting officers shall—

(1) Ensure that the classified acquisition is conducted as required by the NISP or agency procedures, as appropriate; and

(2) Include—

(i) An appropriate Security Requirements clause in the solicitation (see 4.404); and

(ii) As appropriate, in solicitations and contracts when the contract may require access to classified information, a requirement for security safeguards in addition to those provided in the clause (52.204-2, Security Requirements).

(c) *Award phase*. Contracting officers shall inform contractors and subcontractors of the security classifications and requirements assigned to the various documents, materials, tasks, subcontracts,

and components of the classified contract as follows:
(1) Agencies covered by the NISP shall use the Contract Security Classification Specification, DD Form 254. The contracting officer, or authorized representative, is the approving official for the form and shall ensure that it is prepared and distributed in accordance with the ISR.
(2) Contracting officers in agencies not covered by the NISP shall follow agency procedures.

4.404 Contract Clause.
(a) The contracting officer shall insert the clause at 52.204-2, Security Requirements, in solicitations and contracts when the contract may require access to classified information, unless the conditions specified in paragraph (d) of this section apply.
(b) If a cost contract (see 16.302) for research and development with an educational institution is contemplated, the contracting officer shall use the clause with its Alternate I.
(c) If a construction or architect-engineer contract where employee identification is required for security reasons is contemplated, the contracting officer shall use the clause with its Alternate II.
(d) If the contracting agency is not covered by the NISP and has prescribed a clause and alternates that are substantially the same as those at 52.204-2, the contracting officer shall use the agency-prescribed clause as required by agency procedures.

52.204-2 Security Clause Requirements.
As prescribed in 4.404(a), insert the following clause:
Security Requirements (Aug 1996)
(a) This clause applies to the extent that this contract involves access to information classified "Secret."
(b) The Contractor shall comply with—
(1) The Security Agreement (DD Form 441), including the *National Industrial Security Program Operating Manual* (DOD 5220.22-M); and
(2) Any revisions to that manual, notice of which has been furnished to the Contractor.

52.204-2 Security Clause Requirements Continued.
(c) If, subsequent to the date of this contract, the security classification or security requirements under this contract are changed by the Government and if the changes cause an increase or decrease in security costs or otherwise affect any other term or condition of this contract, the contract shall be subject to an equitable adjustment as if the changes were directed under the Changes clause of this contract.
(d) The Contractor agrees to insert terms that conform substantially to the language of this clause, including this paragraph (d) but excluding any reference to the Changes clause of this contract, in all subcontracts under this contract that involve access to classified information.
(End of clause)
Alternate I (Apr 1984). If a cost contract for research and development with an educational institution is contemplated, add the following paragraphs (e), (f), and (g) to the basic clause:
(e) If a change in security requirements, as provided in paragraphs (b) and (c), results (1) in a change in the security classification of this contract or any of its elements from an unclassified status or a lower classification to a higher classification, or (2) in more restrictive area controls than previously required, the Contractor shall exert every reasonable effort compatible with the Contractor's established policies to continue the performance of work under the contract in compliance with the change in security classification or requirements. If, despite reasonable efforts, the Contractor determines that the continuation of work under this contract is not practicable because of the change in security classification or requirements, the Contractor shall notify the Contracting Officer in

writing. Until resolution of the problem is made by the Contracting Officer, the Contractor shall continue safeguarding all classified material as required by this contract.

(f) After receiving the written notification, the Contracting Officer shall explore the circumstances surrounding the proposed change in security classification or requirements, and shall endeavor to work out a mutually satisfactory method whereby the Contractor can continue performance of the work under this contract.

(g) If, 15 days after receipt by the Contracting Officer of the notification of the Contractor's stated inability to proceed, (1) the application to this contract of the change in security classification or requirements has not been withdrawn, or (2) a mutually satisfactory method for continuing performance of work under this contract has not been agreed upon, the Contractor may request the Contracting Officer to terminate the contract in whole or in part. The Contracting Officer shall terminate the contract in whole or in part, as may be appropriate, and the termination shall be deemed a termination under the terms of the Termination for the Convenience of the Government clause.

Alternate II (Apr 1984). If employee identification is required for security or other reasons in a construction contract or architect-engineer contract, add the following paragraph (e) to the basic clause:

(e) The Contractor shall be responsible for furnishing to each employee and for requiring each employee engaged on the work to display such identification as may be approved and directed by the Contracting Officer. All prescribed identification shall immediately be delivered to the Contracting Officer, for cancellation upon the release of any employee. When required by the Contracting Officer, the Contractor shall obtain and submit fingerprints of all persons employed or to be employed on the project.

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.

(i) 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.

(ii) 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.

(iii) 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:

(i) Data Universal Numbering System (DUNS);
(ii) Contract numbers affected unless all contracts by the company are affected;
(iii) Facility CAGE code if the location of the event is different than the prime contractor location;

(iv) Point of contact (POC) if different than the POC recorded in the System for Award Management (address, position, telephone, email);
(v) Contracting Officer POC (address, telephone, email);
(vi) Contract clearance level;
(vii) Name of subcontractor and CAGE code if this was an incident on a subcontractor network;
(viii) Government programs, platforms or systems involved;
(ix) Location(s) of incident;
(x) Date and time the incident was discovered;
(xi) Server names where sensitive information resided at the time of the incident, both at the Contractor and subcontractor level;
(xii) Description of the Government PII and/or SPII contained within the system;
(xiii) Number of people potentially affected and the estimate or actual number of records exposed and/or contained within the system; and
(xiv) Any additional information relevant to the incident.

(g) *Sensitive Information Incident Response Requirements.*

(1) 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.

(2) 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.

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

(i) Inspections,
(ii) Investigations,
(iii) Forensic reviews, and
(iv) Data analyses and processing.

(4) 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:

(i) A brief description of the incident;
(ii) A description of the types of PII and SPII involved;
(iii) A statement as to whether the PII or SPII was encrypted or protected by other means;
(iv) Steps individuals may take to protect themselves;
(v) 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
(vi) 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:

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

(2) 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:

(i) Triple credit bureau monitoring;
(ii) Daily customer service;
(iii) Alerts provided to the individual for changes and fraud; and
(iv) Assistance to the individual with enrollment in the services and the use of fraud alerts; and/or

(3) Establish a dedicated call center. Call center services shall include:

(i) A dedicated telephone number to contact customer service within a fixed period;
(ii) Information necessary for registrants/enrollees to access credit reports and credit scores;
(iii) 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;

(iv) Escalation of calls that cannot be handled by call center staff to call center management or DHS, as appropriate;
(v) Customized FAQs, approved in writing by the Contracting Officer in coordination with the Headquarters or Component Chief Privacy Officer; and
(vi) 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)

ACCESSIBILITY REQUIREMENTS (SECTION 508)

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

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

Section 508 Applicable EIT Accessibility Standards

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

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

36 CFR 1194.24 Video and Multimedia Products, applies to all video and multimedia products that are procured or developed under this work statement. Any video or multimedia presentation shall also comply with the software standards (1194.21) when the presentation is through the use of a Web or Software application interface having user controls available.

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

36 CFR 1194.41 Information Documentation and Support applies to all documents, reports, as well as help and support services. To ensure that documents and reports fulfill the required 1194.31 Functional Performance Criteria, they shall comply with the technical standard associated with Web-based Intranet and Internet Information and Applications at a minimum. In addition, any help or support provided in this work statement that offer telephone support, such

as, but not limited to, a help desk shall have the ability to transmit and receive messages using TTY.

Section 508 Applicable Exceptions

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

Section 508 Compliance Requirements

36 CFR 1194.2(b) (COTS/GOTS products), When procuring a product, each agency shall procure products which comply with the provisions in this part when such products are available in the commercial marketplace or when such products are developed in response to a Government solicitation. Cannot claim a product as a whole is not commercially available because no product in the marketplace meets all the standards. If products are commercially available that meets some but not all of the standards, the bureau must procure the product that best meets the standards. When applying this standard, all procurements of EIT shall have documentation of market research that identify a list of products or services that first meet the bureau's business needs, and from that list of products or services, an analysis that the selected product met more of the accessibility requirements than the non-selected products as required by FAR 39.2. Any selection of a product or service that meets less accessibility standards due to a significant difficulty or expense shall only be permitted under an undue burden claim and requires authorization from the DHS Office of Accessible Systems and Technology (OAST) in accordance with DHS MD 4010.2.

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