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

1. REQUISITION NUMBER FOR180088,OIT186212

PAGE 1 OF 23

2. CONTRACT NO. GS-35F-0115R

3. AWARD/ EFFECTIVE DATE

4. ORDER NUMBER 70SBUR18F00000697

5. SOLICITATION NUMBER 70SBUR18Q00000254

6. SOLICITATION ISSUE DATE 06/19/2018

7. FOR SOLICITATION INFORMATION CALL:

a. NAME Sylwia Salkic

b. TELEPHONE NUMBER *(No collect calls)* 802-872-4134

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: % 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: 541511

SIZE STANDARD: $27.5

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

Office of Information Technology
111 Massachusetts Avenue, NW
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 1240234040000 FACILITY CODE

EXCELLA CONSULTING INC
2300 WILSON BLVD SUITE 630
ARLINGTON VA 222015424

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: 124023404+0000 [redacted]				
	(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: Excella Consulting OFFER DATED 09/13/2018. YOUR OFFER ON SOLICITATION (BLOCK 5), INCLUDING ANY ADDITIONS OR CHANGES WHICH ARE SET FORTH HEREIN, IS ACCEPTED AS TO ITEMS:

30a. SIGNATURE OF OFFEROR/CONTRACTOR

31a. UNITED STATES OF AMERICA *(SIGNATURE OF CONTRACTING OFFICER)*
Kiley Leahy

30b. NAME AND TITLE OF SIGNER *(Type or print)*

30c. DATE SIGNED

31b. NAME OF CONTRACTING OFFICER *(Type or print)*
Kiley Leahy

31c. DATE SIGNED 9/27/18

19. ITEM NO.	20. SCHEDULE OF SUPPLIES/SERVICES	21. QUANTITY	22. UNIT	23. UNIT PRICE	24. AMOUNT
	[redacted]				
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
	[redacted]				
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
	[redacted]				
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
	[redacted]				
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
	Continued ...				

32a. QUANTITY IN COLUMN 21 HAS BEEN

□ RECEIVED □ INSPECTED □ ACCEPTED, AND CONFORMS TO THE CONTRACT, EXCEPT AS NOTED: ____________________

32b. SIGNATURE OF AUTHORIZED GOVERNMENT REPRESENTATIVE

32c. DATE

32d. PRINTED NAME AND TITLE OF AUTHORIZED GOVERNMENT REPRESENTATIVE

32e. MAILING ADDRESS OF AUTHORIZED GOVERNMENT REPRESENTATIVE

32f. TELEPHONE NUMBER OF AUTHORIZED GOVERNMENT REPRESENTATIVE

32g. E-MAIL OF AUTHORIZED GOVERNMENT REPRESENTATIVE

33. SHIP NUMBER

□ PARTIAL □ FINAL

34. VOUCHER NUMBER

35. AMOUNT VERIFIED CORRECT FOR

36. PAYMENT

□ COMPLETE □ PARTIAL □ FINAL

37. CHECK NUMBER

38. S/R ACCOUNT NUMBER

39. S/R VOUCHER NUMBER

40. PAID BY

41a. I CERTIFY THIS ACCOUNT IS CORRECT AND PROPER FOR PAYMENT

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

CONTINUATION SHEET	REFERENCE NO. OF DOCUMENT BEING CONTINUED GS-35F-0115R/70SBUR18F00000697	PAGE 3	OF 23

NAME OF OFFEROR OR CONTRACTOR
EXCELLA CONSULTING INC

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

CONTINUATION SHEET	REFERENCE NO. OF DOCUMENT BEING CONTINUED GS-35F-0115R/70SBUR18F00000697	PAGE 4	OF 23

NAME OF OFFEROR OR CONTRACTOR
EXCELLA CONSULTING INC

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

CONTINUATION SHEET	REFERENCE NO. OF DOCUMENT BEING CONTINUED GS-35F-0115R/70SBUR18F00000697	PAGE 5	OF 23

NAME OF OFFEROR OR CONTRACTOR
EXCELLA CONSULTING INC

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

Section C—Task Order Clauses

This solicitation is subject to the terms and conditions of the GSA Schedule Contract.

Federal Acquisition Regulation (FAR) Clauses incorporated by reference

52.252-2 **Clauses Incorporated by Reference** (Feb 1998)

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

(End of clause)

52.203-19	**Prohibition on Requiring Certain Internal Confidentiality Agreements or Statements**	(Jan 2017)
52.212-4	**Contract Terms and Conditions -- Commercial Items**	(Jan 2017)
52.227-17	**Rights in Data—Special Works**	(Dec 2007)
52.232-39	**Unenforceability of Unauthorized Obligations**	(Jun 2013)
52.237-3	**Continuity of Services**	(Jan 1991)
52.245-1	**Government Property**	(Jan 2017)
52.245-9	**Use and Charges**	(Apr 2012)

Federal Acquisition Regulation (FAR) Clauses incorporated in full text

52.217-8 **Option to Extend Services** (Nov 1999)

The Government may require continued performance of any services within the limits and at the rates specified in the contract. These rates may be adjusted only as a result of revisions to prevailing labor rates provided by the Secretary of Labor. The option provision may be exercised more than once, but the total extension of performance hereunder shall not exceed 6 months. The Contracting Officer may exercise the option by written notice to the Contractor within **30 days before the task order expires.**

(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 task order expiration**; provided that the government gives the contractor a preliminary written notice of its intent to extend at least **60 days** before the contract expires. The preliminary notice does not commit the government to an extension.

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

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

(End of clause)

52.224-3 **Privacy Training – Alternate I (DEVIATION)**

(a) *Definition.* As used in this clause, personally identifiable information means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. (See Office of Management and Budget (OMB) Circular A–130, Managing Federal Information as a Strategic Resource).

(b) The Contractor shall ensure that initial privacy training, and annual privacy training thereafter, is completed by contractor employees who—

(1) Have access to a system of records;

(2) Create, collect, use, process, store, maintain, disseminate, disclose, dispose, or otherwise handle personally identifiable information on behalf of an agency; or

(3) Design, develop, maintain, or operate a system of records (see also FAR subpart 24.1 and 39.105).

(c) The contracting agency will provide initial privacy training, and annual privacy training thereafter, to Contractor employees for the duration of this contract. Contractor employees shall satisfy this requirement by completing *Privacy at DHS: Protecting Personal Information* accessible at *http://www.dhs.gov/dhs-security-and-training-requirements-contractors*. Training shall be completed within 30 days of contract award and be completed on an annual basis thereafter not later than October 31st of each year.

(d) The Contractor shall maintain and, upon request, provide documentation of completion of privacy training to the Contracting Officer.

(e) The Contractor shall not allow any employee access to a system of records, or permit any employee to create, collect, use, process, store, maintain, disseminate, disclose, dispose or otherwise handle personally identifiable information, or to design, develop, maintain, or operate a system of records unless the employee has completed privacy training, as required by this clause.

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

(1) Have access to a system of records;

(2) Create, collect, use, process, store, maintain, disseminate, disclose, dispose, or otherwise handle personally identifiable information; or

(3) Design, develop, maintain, or operate a system of records.

(End of clause)

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" wherever such application is appropriate. Use of the word "solicitation" is understood to mean "fair opportunity notice" wherever such application is appropriate.

(End of clause)

52.252-6 **Authorized Deviations in Clauses** (Apr 1984)

(a) The use in this solicitation or contract of any Federal Acquisition Regulation (48 CFR Chapter 1) clause with an authorized deviation is indicated by the addition of "(DEVIATION)" after the date of the clause.

(b) The use in this solicitation or contract of any clause with an authorized deviation is indicated by the addition of "(DEVIATION)" after the name of the regulation.

(End of clause)

Homeland Security Acquisition Regulation (HSAR) Clauses incorporated by reference

The full text of HSAR clauses and provisions may be accessed electronically at the following internet address: http://farsite.hill.af.mil/vfhsara.htm

3052.203-70	**Instructions for Contractor Disclosure of Violations**	(Sep 2012)
3052.205-70	**Advertisements, Publicizing Awards, and Release**	(Sep 2012)

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

3052.204-71 **Contractor Employee Access, Alternate I** (Sep 2012)

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

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

(2) Sensitive Security Information (SSI), as defined in Title 49, Code of Federal Regulations, Part 1520, as amended, "Policies and Procedures of Safeguarding and Control of SSI," as amended, and any supplementary guidance officially communicated by an authorized official of

the Department of Homeland Security (including the Assistant Secretary for the Transportation Security Administration or his/her designee);
(3) Information designated as "For Official Use Only," which is unclassified information of a sensitive nature and the unauthorized disclosure of which could adversely impact a person's privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national or homeland security interest; and
(4) Any information that is designated "sensitive" or subject to other controls, safeguards or protections in accordance with subsequently adopted homeland security information handling procedures.
(b) "Information Technology Resources" include, but are not limited to, computer equipment, networking equipment, telecommunications equipment, cabling, network drives, computer drives, network software, computer software, software programs, intranet sites, and internet sites.
(c) Contractor employees working on this contract must complete such forms as may be necessary for security or other reasons, including the conduct of background investigations to determine suitability. Completed forms shall be submitted as directed by the Contracting Officer. Upon the Contracting Officer's request, the Contractor's employees shall be fingerprinted, or subject to other investigations as required. All Contractor employees requiring recurring access to Government facilities or access to sensitive information or IT resources are required to have a favorably adjudicated background investigation prior to commencing work on this contract unless this requirement is waived under Departmental procedures.
(d) The Contracting Officer may require the Contractor to prohibit individuals from working on the contract if the Government deems their initial or continued employment contrary to the public interest for any reason, including, but not limited to, carelessness, insubordination, incompetence, or security concerns.
(e) Work under this contract may involve access to sensitive information. Therefore, the Contractor shall not disclose, orally or in writing, any sensitive information to any person unless authorized in writing by the Contracting Officer. For those Contractor employees authorized access to sensitive information, the Contractor shall ensure that these persons receive training concerning the protection and disclosure of sensitive information both during and after contract performance.
(f) The Contractor shall include the substance of this clause in all subcontracts at any tier where the subcontractor may have access to Government facilities, sensitive information, or resources.

(End of clause)

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 removing or 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 remove or replace personnel or facilities until the Contracting Officer approves the change.

[redacted]

(End of clause)

Safeguarding Of Sensitive Information (Mar 2015)
(HSAR Class Deviation 15-01)
(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 107296, 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)
(HSAR Class Deviation 15-01)
(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)

Other Clauses

Option for Additional Teams

At any time during the life of the contract, the Government may require the performance of the numbered line items identified in the Schedule as an optional team, in the quantity and at the price stated in the Schedule. If exercised, these optional team options will be month to month, using monthly pricing for the options. The Contracting Officer may exercise the optional team options by written notice to the Contractor within 15 days. Exercise of the optional team option line items does not increase the total task order value.

Other Task Order Requirements

C-1. 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
(802) 288-7600

C-2. 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.

C-3. POSTING OF ORDER IN FOIA READING ROOM

(a) The government intends to post the order resulting from this notice to a public FOIA reading room.

(b) Within 30 days of award, the contractor shall submit a redacted copy of the executed 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.

[redacted]

[redacted]

C-5. 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 order 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.

C-6. Government-Furnished Property

(a) The Government will provide contractor personnel with the GFP specified in PWS Section 8.3.

(b) The contractor shall notify personnel that there shall be no expectation of privacy on any USCIS Systems.

(c) The contractor shall operate Government provided property in accordance with USCIS procedures and manufacturer's specifications.

(d) The contractor shall initiate and track maintenance calls and/or service requests for government provided IT equipment to the DHS Helpdesk. The contractor shall notify the COR and/or Program Manager (PM) of any repair needs and/or problems with maintenance/service contractor activities within four (4) hours of each occurrence.

(e) The Government provides computer laptops and software in various hardware configurations, and reserves the right to upgrade, add, delete, or replace equipment and software.

Section D—List of Attachments

Attachment	Title/Description	Pages
1	Performance Work Statement (PWS)	17
2	Security Requirements	8
3	DHS Enterprise Architecture Compliance	1
4	Capitalized Property, Plant & Equipment (PP&E) Assets Internal Use Software (IUS)	2
5	Section 508 Compliance	2
[redacted]	[redacted]	[redacted]

Performance Work Statement
United States Citizenship and Immigration Services (USCIS)
Risk and Fraud Analytics and DevSecOps (RFAD)

1. OVERVIEW

Risk and Fraud Analytics and Development, Security and Operations (DevSecOps) (RFAD) will consist of teams to provide data analytics and DevSecOps services to support USCIS Information Technology (IT) system delivery. The USCIS RFAD teams will perform data analytics and DevSecOps services for USCIS systems hosted in any of the USCIS datacenters or cloud environments. Currently, that environment is located in Amazon Web Services (AWS) but may eventually be located in a different cloud environment. The RFAD teams will provide data science driven solutions as required but including for example, text analytics, data analytics and entity relationship analysis in order to identify and detect fraud and national security concerns. The team will also develop a graphical user interface and search capability to be used with the text analytics platform developed under the auspices of this contract.

The Government will oversee the architecture and design of the IT capabilities, the Agile methodologies to be used, product planning, and the flow of requirements. The RFAD contractor will be responsible for developing high-quality IT capabilities working within those architectures and processes to meet the business requirements.

2. SCOPE

The contractor will engage in many different experiments, projects, and/or efforts to accomplish the following goals: (1) Establish big data reporting and an enterprise analytics platform that will enable USCIS to analyze increasingly larger and more complex data sets. This analysis includes developing machine learning algorithms, and natural language processing (NLP) to improve how USCIS predicts fraud and processes information to meet USCIS mission needs. (2) Identify and correct data quality issues and establish a data governance framework to enforce data standards and improve accuracy using integrated internal and external disparate data sources. (3) Develop highly optimized, scalable automatic case matching logic on microservice/container technology. (4) Develop a graphical user interface which will allow USCIS personnel to interact with text analytics oriented fraud identification systems. (5) Provide other data science and data analytics solutions to meet agency needs. As needed, the contract teams will support the agency for other data science capabilities that require machine learning, artificial intelligence or automated data models to scientifically prove data facts and create automated features for the business based on models.

USCIS will manage system roadmaps, project plans, and product and release backlogs that will be the basis for the contractor's work and the contractor will support as needed. A USCIS Product Owner will specify high-level requirements to this and other contractors' Agile teams. As in typical Agile processes, USCIS subject matter experts (SMEs) will work together with the RFAD teams to define user stories and establish acceptance criteria. These acceptance criteria will specify expected functionality for a user story, as well as any non-functional requirements that must be met in the development of the story. The USCIS Product Owner, supported by SMEs and business analysts, will determine whether or not acceptance criteria have been satisfied. USCIS may adopt various Agile processes such as, but not limited to, Extreme Programming (XP), SCRUM, Kanban, and Lean Software Development, and the contractor will be expected to conform its processes to these approaches.

The RFAD teams will provide data analytics capacity, to include, at a minimum, the ability to perform fraud detection, monitoring and compliance and to fix data by leveraging new tools in Big Data Analytics Platforms for USCIS. The team will include "full stack" expertise and will have the full set of responsibilities for data analytics, development, operations, security, and testing of a set of capabilities in development, test, stage and production environments. The term expert or expertise is used throughout this document. An expert is defined as a person who has comprehensive and authoritative knowledge of, or skill in, a particular area. Examples of expertise are where an individual has published technical whitepapers on the subject or given technical presentations at IT conferences on the subject. The contractor will use a Continuous Integration / Continuous Delivery (CI/CD) approach and is expected to adopt cutting edge best practices for IT delivery.

Critical elements of the RFAD team will be:

- High productivity
- High quality work
- High level of initiative and ownership
- Collaboration and cooperation with other USCIS teams and participants
- Technical skills and expertise as necessary (See Technical Landscape Table and Key Personnel requirements)
- Estimation and planning skills
- Innovation and creativity in problem solving

As DHS requires Section 508- compliant user interfaces, the contractor shall accredit at least one person for every 2 teams as a Section 508 DHS Trusted Tester. This individual must be properly vetted and certified at the start of the contract. The contractor shall adopt evolving USCIS design and coding standards in the course of application development. The contractor shall provide technical methods, techniques, and concepts that are innovative, practical, cost-effective, and conducive to Agile application development. The contractor shall develop IT capabilities based on requirements that are evolving and emerge as the business climate shifts.

The contractor will be required to develop high quality code and is responsible for any technical debt that is incurred as a result of their development activities. The contractor shall balance core productivity with technical debt, and should never trade off quality in favor of productivity. Technical debt should be addressed as it occurs and should not become so overwhelming that it must be addressed using an entire or several entire sprints.

Services in support of RFAD shall be provided by personnel with demonstrated experience in using USCIS specified tools and technologies as described in section *2.1 Technical Landscape*. Each team shall collectively be experienced with all tools and technologies. DevSecOps involves some degree of analysis, requirements collection, design, development, test, platform engineering, and production operations in addition to the support functions of configuration management, planning, and project management. In addition, DevSecOps should be considered to be "infrastructure as code" with the mindset and practice of automating through code everything possible. The specific tasks applicable under this task order are detailed in section 4 *TASKS.* Delivery and operation will follow Agile and DevSecOps industry best practices.

2.1 Technical Landscape

The contractor shall use USCIS enclaves in the Amazon Web Services (AWS) public cloud, Department of Homeland Services (DHS) private cloud, and/or other cloud environments specified by the Government, for development, testing, and production.

The USCIS technical landscape is shifting from a proprietary COTS-based framework to open source. One of USCIS's goals is to use platforms and tools that are familiar to a broad range of developers; this has influenced the selection of open source products and frameworks. All USCIS source code and tests are stored in the agency's Enterprise GitHub repository, and code is shared between different projects where appropriate. USCIS is also moving towards containerized micro-service architecture. The contractor shall provide expertise in this arena.

The RFAD task order will use the USCIS standard platform and tools. This platform will evolve over time to continue to fit the needs of USCIS and the contractor will be expected to support an ever evolving tool stack. The current platform is described in the chart below:

Table 1: Current Tool Suite and Platforms/Name	Function
AWS Cloud	Public cloud platform. USCIS currently uses EC2, S3, ECR, EMR, RedShift, RDS, CloudFormation, Lambda, Dynamodb, Neptune and a number of other AWS services
Amazon Linux (RHEL)	Operating System
Apache ActiveMQ	Messaging Provider
Apache Commons Libs	Java software library
Apache Jmeter	Performance testing
Apache Tomcat	Application server
Apache Hive	A data warehouse software project built on top of Apache Hadoop for providing data summarization, query and analysis.
Apache Spark	Apache Spark is an open-source cluster-computing framework
Apache Hadoop	A collection of open-source software utilities that facilitate using a network of many computers to solve problems involving massive amounts of data and computation.
Logstash	an open source data collection engine with real-time pipelining capabilities.
Apache Sqoop	a tool designed for efficiently transferring bulk data between Hadoop and structured datastores such as relational databases.
Cassandra	Database
CentOS	Operating System
Chaos Monkey	Application Resiliency Tool

Chef	Deployment scripting
Cucumber/Jasmine/Selenium	Integration Testing
Customer Care Desktop	UII framework
DeQue FireEyes	508 Development Test tool
Docker	Containerization
Elasticsearch	A distributed, multitenant-capable full-text search engine
Elastic.co Kibana	An open source data visualization plugin for Elasticsearch.
Fortify	Security test tool
Git / Enterprise GitHub	Distributed version control
Hibernate 4	ORM Database integration
iText	PDF file generation
Jackson	Java Representation of JSON
Java	Programming Language
Java Mail	Email message generation
JAXB	Java Representation of XML
Jenkins	Continuous integration server
Jira	Agile lifecycle management tool
JUnit	Java Unit testing library
Liquibase	Database automation
Maven	Java artifacts and dependency managements framework
Neo4J	Graph Database
New Relic	Application and Infrastructure Monitoring
Nexus	Repository manager
Oracle & PL/SQL	Database/Reporting
PostgreSQL	Database
Python / Anaconda	Programming Language / Statistical Analysis Packages
R / R Studio	Statistical Analysis Software
Rails	Web development framework
rspec	Unit Testing
Ruby	Programming Language
SAS	Statistical Analysis Software
SiteMesh	Java web application framework
SoapUI	WebService Testing tool
Spring Framework	Application Framework
Ubuntu	Operating System
Windows Server	Operating System
BouncyCastle (FIPS)	Crytography API
Kafka	Message Streaming Platform
Snap	Continuous integration and delivery platform
Spark/Scala	Hadoop platform and corresponding programming language
Artifactory	Repository manager
HashiCorp Terraform	Cloud resource creating and management tool
OpenShift	Container Platform

3 TEAMS

The contractor shall provide DevSecOps Data Science and DevSecOps UI/UX teams to perform the tasks as described in the following sections, with expert level ability in the technologies stated in section 2.*1 Technical Landscape.* The team structure shall adhere to the following requirements:

- **Program Management Team** – To include three (3) staff members, including a Program Manager Senior Level, a Solutions Architect/DevSecOps Architect Senior Level, and a Chief Data Architect/ Data Scientist Senior Level, that will work with the DevSecOps teams to deliver the required services. All members of the Program Management team will be key personnel.

- **DevSecOps Data Science Teams** – Twelve (12) person teams that each include a Scrum Master, a Business Analyst, a Senior Database Architect/Administrator and a mix of developers, data scientists and cloud engineers.

- **DevSecOps User Interface (UI)/User Experience (UX) Team** – Six (6) person team which includes a Scrum Master / Business Process Analyst, a UI/UX lead designer Senior Level (Key Personnel), and a mix of developers and cloud engineers.

- **Optional DevSecOps Data Science Teams** – Twelve (12) person teams that each include a Scrum Master, a Business Analyst, a Senior Database Architect/Administrator and a mix of developers, data scientists and cloud engineers.

- **Optional DevSecOps UX/UI Team** – Six (6) person team which includes a mix of cloud engineers and senior developers/testers.

All personnel shall be full time, part-time personnel are not permitted.
Each team is not required to have the same mix of labor categories. All personnel shall be mid-level to senior level labor categories. The contractor shall determine the labor mix for each team to provide the best overall solution to the government.

The purpose of the teams is to provide data science driven solutions, application development, UI/UX design and web interface buildout for view/search capabilities, operations, security, and testing requirements. The contractor should use a test driven development (TDD) approach. The contractor's work shall conform to the architecture and design provided by USCIS and the Agile processes set up by USCIS, but this work will be managed by the contractor teams. The teams must have all of the skills necessary to perform the tasks indicated in Section 4. It is important that the contract personnel assigned to the task order as a whole have the skills necessary for development, operations, security, test, and maintenance, but that does not mean that specific team members must be designated as testers, coders, etc. Most of the team members should have more than one skill, for example. It is up to the contractor to structure the teams so that it can provide all of the necessary functions at a high level of productivity and quality. The teams should be experienced with the latest systems development technologies and programming languages and the AWS cloud.

The Contractor must provide a DHS OAST Trusted Tester certified to current test standards for every two teams of developers that creates Information and Communications Technology (ICT), or content to be hosted on ICT, within 90 days of award. To clarify, for every two DevSecOps teams, there must be at least one certified DHS OAST Trusted Tester, in accordance with Section 508 compliance (see Attachment 5). When standards change and re-certification is required by DHS OAST then the Contractor must ensure that all Trusted Testers re-certify within 90 days of training availability. The Contractor must provide a quarterly report that lists the contract name, number, and COR with each Trusted Tester's name, certification level, certification date, certification number, E-mail address, phone number, and supported projects to the COR and USCIS Section 508 Coordinator. This report must also be provided within 10 working days of any change in the Trusted Tester population. The DHS Office of Accessible Systems and Technologies (OAST) administers the certification training and test. You can find their site here: http://dhsconnect.dhs.gov/org/comp/mgmt/cio/oast/Pages/default.aspx.

The trusted tester duty should be considered an ancillary role for the team member who is provided to meet this requirement.

4 TASKS

4.1 Development

- Contractor shall be responsible for performing the full suite of DevSecOps tasks using Agile methodologies, including participating in creating user stories for business functionality and technical requirements and defining acceptance criteria
- Contractor shall be responsible for estimating the size of stories, designing solutions, developing code and automated tests, creating deployment scripts, managing code in production, and managing any Database solutions.
- Contractor shall test its product and ensure its quality, and shall deploy its code.

4.2 Documentation

- Contractor shall assist in the documentation of user stories, acceptance criteria and tasks to be completed to fulfill the definition of done for a story.
- Contractor shall document system design and procedures in the wiki that USCIS uses for a System Design Document (SDD) concurrent with development activities. In general, USCIS prefers relatively lightweight but effective and usable documentation.

4.3 Design

- Contractor shall participate in the design of technical solutions to meet the business need, working within standards defined by USCIS and subject to review by the agency.

- Contractor will be responsible for designing and implementing user interfaces and for working with users to maximize the usability of the system. Design will be done in conformance with USCIS design standards and in collaboration with USCIS.

4.4 Test and Integration

Testing shall primarily be automated, reflecting the best-practice "testing pyramid" with an emphasis on excellent code coverage through unit tests. Unit test should cover a minimum of 85% of the code and the contractor shall provide at least monthly reporting on code coverage and technical debt to the government. The build pipeline will also include USCIS standard tools for code standards, test coverage, security testing, and Section 508 Compliance.

- Contractor shall be responsible for creating test cases and automated test scripts to support test automation activities.
- Testing shall primarily be automated, reflecting the best-practice "testing pyramid" with an emphasis on excellent code coverage through unit tests. Unit test should cover a minimum of 85% of the code and the contractor shall provide at least monthly reporting on code coverage and technical debt to the government. The build pipeline will also include USCIS standard tools for code standards, test coverage, security testing, and Section 508 Compliance.
- The contractor's code shall meet the functional and non-functional requirements, and the automated and manual tests performed shall verify that it does so. Code and tests will be reviewed by USCIS OIT Independent Validation & Verification (IV&V) to ensure that the testing is appropriate, adequate, effective, and that it mitigates key risks.
- Contractor shall use CI/CD techniques. Code should be deployed to production at least weekly, with preference of daily releases to production in small change sets. The system should be deployable at any time.
  - Contractor shall deploy features such that the government can decide when the features will be activated.
  - Contractor shall assist with crafting validation steps (both positive and negative testing) for user acceptance testing on an as needed basis.
- Contractor shall perform security scans and automated testing with each build to support ongoing authorization and continuously improved security posture.
- Contractor shall perform automated load and performance testing with every deployment. In addition, the contractor shall provide a mechanism or manage the mechanism to provide regular reporting on application performance.
- Contractor shall perform automated integration testing with all external connections and applications.

4.5 Operations

- Contractor shall be responsible for the operation in production of the capabilities they develop.
- Contractor shall build in monitoring triggers to effectively reveal production issues in a timely fashion.
- Contractor shall provide root cause analysis on all outages with actionable

recommendations on how to prevent issues going forward.

- Contractor shall ensure that the system is monitored effectively to reveal any production issues when they occur and to monitor the performance of the application.
- Contractor shall ensure that the systems are monitored effectively to reveal user analytics and interactions and provide the capability to automatically report on such activities.
- Contractor shall ensure that there is an automated method to monitor for network-related production issues, providing the capability to rule out application issues.
- Primary responsibility for monitoring production systems is held by the USCIS Network Operations Center (NOC). The contractor shall ensure that appropriate monitoring is in place and shall work with the USCIS NOC on monitoring alerts and escalation processes.
- While USCIS expects the quality of the development to not require it, in the event of a critical or high severity production issue, the contractor shall be available to restore system availability and functionality 24 hours a day, seven days a week (24x7).

4.6 Administrative Activities

- The contractor shall collaborate with stakeholders, support contractors, and third party vendors regarding system integration, performance, security, Section 508, system acceptance, user acceptance, usability, and test and evaluation reporting.
- The contractor shall manage all contractor resources and supervise all contractor staff in the performance of work on this task order. The contractor shall manage and coordinate its team(s) on a day-to-day basis and ensure plans are communicated to team members.
- The contractor shall organize, direct and coordinate planning and execution of all task order activities.
- Vehicles for transparency, such as the agency Agile Application Lifecycle Management (ALM) tool, shall be maintained with data so that reports and charts can be generated as needed, and so that user stories, defects, tasks and their status are available to stakeholders. Task boards and collaboration sites, meetings, and demos can be used to share information and report progress.

5 KEY PERSONNEL

The contractor shall identify key personnel and provide statements of qualifications for these individuals. This task order requires four (4) key personnel: a Program Manager, a Solutions Architect/ DevSecOps Architect, a Chief Data Architect/ Data Scientist and a UI/UX Lead Designer/Subject Matter Expert. The Program Manager shall be a current, full time employee of the prime contractor. All other key personnel shall be current, full time employees of the prime contractor or a subcontractor. These individuals must have extensive expertise in the Agile and DevSecOps approaches, and experience using many of the tools included in the Development/Test Tool Suite identified in section 2.1 *Technical Landscape*. Since this is a team-oriented contract, all of the key personnel may have other duties that coincide with their skillsets, such as business analyst, development, and Scrum Master functions.

The Program Manager shall ensure that all work on this contract complies with contract terms and conditions and shall have access to contractor corporate senior leadership when necessary. The Program Manager shall be the primary interface with the USCIS Contracting Officer's Representative (COR) and Contracting Officer (CO) and shall attend status meetings and ad hoc meetings with stakeholders as required, accompanied by other key personnel when necessary.

Key Personnel Minimum Qualifications:

- **Program Manager Senior Level**
    - Shall have a minimum of ten (10) years of IT Project Management experience focusing on development projects, of which two (2) years experience shall be in managing IT DevSecOps projects specifically.
    - Shall have a current Project Management Professional (PMP) Certification from PMI.
    - Shall at a minimum have a Bachelor's degree in Computer Science, Information Technology Management or Engineering, or other IT related degree **or** two (2) additional years of experience in IT Project Management in lieu of a degree for a total of twelve (12) years of experience.
    - Shall have experience managing scrum team(s).

- **Solution Architect/DevSecOps Architect Senior Level**
    - Shall have a minimum of ten (10) years of experience in the Information Technology field focusing on development projects, DevSecOps and technical architecture, of which three (3) years shall be in architecture & design deploying enterprise applications in cloud platforms, preferably in AWS.
    - Shall have, at a minimum, a Bachelor's degree in Computer Science, Information Technology Management or Engineering, or other IT related degree **or** two (2) additional years of experience in the Information Technology field in lieu of a degree for a total of twelve (12) years of experience.
    - Shall possess expertise in large scale, high performance enterprise big data application deployment and solution architecture on complex heterogeneous environments in AWS.

- **Chief Data Architect/ Data Scientist Senior Level**
    - Shall have at least fifteen (15) years of experience in enterprise data architecture, of which five (5) years of experience shall be in Conceptual/Logical/Physical data modeling **and** Relational and Dimensional Data Modeling.
    - Shall have experience in modeling solutions in AWS
    - Must have a strong understanding of cloud architecture, specifically AWS, as it relates to data processing (i.e., EC2, S3, Redshift, etc.)
    - Must be able to define & maintain BI/Data Warehouse methodologies, standards, and industry best practices

  - Shall have experience leading and architecting enterprise wide initiatives, specifically system integration, data warehouse build, data mart build, data lakes, etc. for a large enterprise
  - Shall have experience briefing the benefits and constraints of technology solutions to technology partners, stakeholders, team members, and senior levels of management
  - Shall have, at a minimum, a Bachelor's degree in data science, engineering, statistics.

- **UI/UX Design Lead Senior Level**
  - Shall have a minimum of eight (8) years of experience in the Information Technology field focusing on development projects and UI/UX Design specifically, of which three (3) years shall be in architecture & design providing UI/UX Design expertise for enterprise applications.
  - Shall possess expertise in a large scale, high performance enterprise application deployment and UI/UX Design on complex heterogeneous environments in AWS.
  - Shall have a Bachelor's degree or two (2) additional years of experience in the Information Technology field in lieu of a degree for a total of ten (10) years of experience.

6 TRANSITION SUPPORT

Upon completion of performance of this task order, the contractor shall fully support the transition of work that is turned over to another entity, either government or a successor offeror(s). The contractor shall assist with transition. To help ensure smooth transition, it is expected that the incoming and outgoing contractors will use techniques such as pair programming to facilitate knowledge sharing without disrupting development.

Because the contractor will have automated the development, test, and deployment pipeline, and because the contractor will have documented important design decisions and processes in the SDD, the expectation is that this automation and documentation will be utilized to enable a smooth transition.

The contractor shall be responsible for the implementation of the transition and application cutover activities. The transition shall cause no disruption in development services. To ensure the necessary continuity of services and to maintain the current 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. As part of the transition, the contractor shall be responsible for:

- Inventory and orderly transfer of all GFP, to include hardware, software, and licenses, Contractor Acquired Government Property, and Government Furnished Information

(GFI)

- Transfer of documentation currently in process
- Transfer of all software code in process
- Certification that all non-public DHS information has been purged from any contractor- owned system
- Exchange of accounts to access software and hosted infrastructure components
- Participation in knowledge transfer activities in accordance with the transition plan
- Providing members to participate in transition of management team

Transition planning generally begins 120 days before the transition deadline. If the government provides a Transition Plan template, the contractor shall complete it as assigned; otherwise the contractor shall submit a Transition Plan at the direction of the government. The Transition Plan shall:

- Document the strategic approach
- Identify equipment, hardware, software, documents and other artifacts that are included in the transition
- Establish milestones and schedules
- Establish activities
- Identify transition risks and risk mitigation
- Define roles and responsibilities
- Define transition approval authorities and lines of communication
- Define appropriate labor mix to perform CI/CD activities
- Define a knowledge transfer approach
- Define a property inventory and transition approach
- Create bi-party or tri-party agreements
- Provide checklists

7 DELIVERABLES

The primary deliverable of this task order is deployed application code. The contractor shall deliver this code throughout the period of performance. Deployed application code is defined as:

- Application Source Code
- Application Build Scripts
- Test Code/Test Cases
- Environment Build Scripts
- Deployment Scripts

All deployed application code shall be checked into the enterprise source code repository. Please note that the test code for automated tests is a critical deliverable: USCIS expects high test code coverage (a minimum of 85% unit test code coverage) and effective tests, as these will become part of the regression test suite to be used in future development work as well.

The contractor shall deliver system design documentation on the Software Design Document wiki, as well as scripts for manual testing when appropriate.

The contractor shall submit electronic copies of document deliverables to the CO and COR (and others as specified by the CO or COR) via e-mail in the format specified in the table below. All document deliverables shall be made by close of business (COB) 4:30pm ET Monday through Friday, unless stated otherwise.

All deliverables submitted in electronic format shall be free of any known computer virus or defects. If a virus or defect is found, the deliverable will not be accepted. The replacement file shall be provided within two (2) business days after notification of the presence of a virus.

7.1 Task Order Management Artifacts

The contractor shall provide reports such as status briefings that support task order management, as described below.

As required by the COR, the contractor shall attend meetings with the COR and/or other USCIS stakeholders in order to review work accomplished, work in progress, plans for future work, transition plans and status, and issues pertinent to the performance of work tasks that require USCIS attention.

In the event the government requires additional information related to contract technical or schedule performance, risks, resources, or any contract-related data, the contractor shall provide this report information in the format requested by the government. Requests for reporting may vary in scope and complexity and may require the contractor to attend OIT meetings to obtain required information, review and research applicable documentation, and extract applicable database information required to assemble the report.

7.2 Deliverables Schedule

The deliverables that apply to this task order, and that the contractor shall provide, are outlined in *Table 2: Deliverables Schedule.*

Table 2: Deliverables Schedule

PWS location	Item	Frequency of Delivery	Acceptable Formats
3	Section 508 DHS Trusted Tester certification	Within 90 days of award, or when standards change and re-certification is required by DHS OAST, re-certification for all Trusted Testers within 90 days of training availability.	Email Attachment to COR and CS/CO.

3	Trusted Tester Report	Quarterly or within 10 days of any change in the Trusted Tester population.	MS Word, Excel
4	In-process application code, test code/test cases deployment scripts, build scripts	Continuously, with each build	Code checked into the USCIS code repository
4	Shippable application code, test code/test cases deployment scripts, build scripts	Continuously, with each commit	Code checked into the USCIS code repository
4	System Design Document (SDD)	Continuously updated	Wiki
4	Sprint Review Brief (includes burndown chart, unit testing code coverage, technical debt)	Every two weeks during Sprint Review	PowerPoint, MS Word, Excel, Visio
4	Web Services Logs, ICD and other related deliverables	As directed	MS Word, Excel, Visio or PowerPoint
6	Transition Out Plan	120 days prior to expiration of the TO or as directed	MS Word 2010-or other as directed by government
7.1	Status Briefings, such as presentations, database extractions, meeting reports, burndown charts, etc.	As directed	MS Word, Excel, Visio, or PowerPoint
7.1	Staffing Report (includes departed staff and open billets and status) to COR and ITPM	Weekly for base year and then at least monthly thereafter	PowerPoint, MS Word, Excel, Visio
7.1	Contract Status Report (covers actions completed on each task for time period)	As directed by the Government	PowerPoint, MS Word, Excel, Visio
7.1	Quality Management Plan, Test & Evaluation, Management Plan, and Configuration Management Plan. These plans will be identified and requested on a case by case basis as they pertain to a project or the task order as a whole.	As directed by the government	MS Word or other, as directed by government

8.1	Corporate Telework Plan	As directed	MS Word 2010-or other as directed by government
8.3	GFP Inventory (must contain CIS ID number, location, name of contactor holding equipment, date)	Monthly	Excel
9.0	Draft Quality Assurance Surveillance Plan	Within 30 days of task order award	MS Word
N/A	Separation Notification	The CO and COR must be notified of each contract employee termination/resignation. (The COR will then notify the Office of Security & Integrity (OSI) Personnel Security Division (PSD) to coordinate the exit clearance forms.	Within five (5) days of each occurrence.
N/A	Redacted copy of the executed task order including all attachments suitable for public posting under the provisions of the Freedom of Information Act (FOIA)	Within 30 days of task order award	Email to foiaerr.nrc@uscis.dhs.gov with a courtesy copy to the CO.

7.3 Inspection and Acceptance

Various government stakeholders will inspect contractor services and deliverables. The CO will provide official notification of rejection of deliverables. Inspection and acceptance of deliverables will use the following procedures:

- The government will decide whether to accept functionality delivered after it is demonstrated to a government product owner. The product owner and other stakeholders might provide feedback that requires re-work on the contractor's part. This process follows normal Agile software development practices. Feedback and government acceptance will be provided according to the standard agile practice; however, due to the nature of the work, it is possible that re-work could be determined after a release goes out and is accepted if a noticeable issue is determined after it is put into production.
- The government will also periodically evaluate the contractor's code quality, test coverage, test and deployment code quality, security, and so on. Based on these periodic reviews, the government may require rework on the contractor's part. The government expects high quality work that meets standards specified by the

government, and does not expect to find significant problems during these reviews.

8 TASK ORDER ADMINISTRATION DATA

8.1 Place of Performance

The principal place of performance shall be at the contractor provided work site. The government is amenable to remote workers as long as the work is completed efficiently and effectively. Up to 40% of each team is able to work remotely. Key Personnel is not allowed to work remotely. If remote work and/or telework will be utilized, then the contractor shall provide remote work and and/or telework plans for approval by the government. The contractor facility shall be in close proximity to the USCIS facility at 111 Massachusetts Ave NW, Washington D.C., not to exceed a distance of 20 miles. Meetings will take place at both the contractor site and USCIS offices in the Washington, D.C. Metropolitan Area, including, but not limited to 20 Massachusetts Avenue, N.W., and 111 Massachusetts Avenue, N.W., Washington D.C. If indicated by the government, meetings may also occur at the contractor's work site, especially when close collaboration between stakeholders and the development team is needed. The contractor shall provide workspace, such as a conference room, to accommodate up to six government representatives.

8.2 Hours of Operation

Normal duty hours for the Government are from 8:00am to 5:00pm, Monday through Friday, excluding Federal Government holidays. The contractor shall be available during this time period, but also available to support any outages to the systems on a 24x7 basis. It is the expectation of the government, that the systems are built in such a way, that they do not go down and therefore this support should be minimal.

8.3 Government Furnished Property (GFP)/Government Furnished Information (GFI)

Laptops, mobile phones and PIV cards will be issued as GFP and used in performing work on this contract. No personal or company owned storage devices, (thumb drives, DVDs, or CDs) shall be used with the GFP. A webinar account, such as AT&T Connect, will be provided to the contractor to facilitate virtual demos and other meetings with stakeholders at various physical locations. Mobile devices may be provided as identified by the COR or Government Program Manager.

GFI, such as USCIS design standards, will be provided to the contractor following award.

Table 3: Government Furnished Property

Equipment / Government Property	Date / Event Indicate when the GFP will be furnished	Date / Event Indicate when the GFP will be returned	Unit	Quantity	Serial Number(s)	Manufacture & Model Number

Laptop Windows Based and MACs	After EOD	Upon Departure	EA	All contract personnel	TBD	Windows HP 820 G4 13 in screen Mac Pro A1398 15 in screen
PIV Card	After EOD	Upon Departure	EA	All contract personnel	TBD	Standard USCIS approved manufacturer
Mobile Phone	After EOD	Upon Departure	EA	All key personnel	TBD	Samsung Galaxy or an Apple iPhone

The contractor is responsible for all costs related to making the property available for use, such as payment of all transportation, installation or rehabilitation costs. The contractor will be responsible for receipt, stewardship, and custody of the listed GFP until formally relieved of responsibility in accordance with FAR 52.245-1 Government Property and FAR 52.245-9 Use and Charges. The property may not be used for any non-task order purpose. The contractor bears full responsibility for any and all loss of this property, whether accidental or purposeful, at full replacement value.

8.4 Government Directed Travel

Travel may be required in order to perform certain tasks assigned by the government. The contractor shall be reimbursed for travel in accordance with the GSA Federal Travel Regulations, 41 Code of Federal Regulations (CFR), and Chapters 300 through 304. The contractor shall be responsible for obtaining COR approval (email is acceptable) for all reimbursable travel in advance of each travel event. The travel request should summarize the purpose of travel, dates, per diem, hotel and airline costs. The contractor may not be compensated for unapproved travel requests.

Upon completion of travel, all documentation associated with the respective travel shall be submitted with the invoices. 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 USCIS offices located at 111 Massachusetts Ave NW, Washington D.C. Home to work travel is not reimbursable.

9 PERFORMANCE CRITERIA

A Balanced Scorecard approach will be used to evaluate contractor performance. The contractor teams will be evaluated every four weeks and the evaluation will be discussed with the contractor. The purpose of the scorecard and discussions is to enhance performance. In addition, in the aggregate, the scorecards and discussions will be used partially as a basis for past performance reporting.

The relative weights of the evaluation categories will be adjusted by the Government based on its experiences, and will be communicated to the contractor after each monthly cycle. The contractor and the CO will receive a copy of the evaluation. The contractor may provide comments or responses to the scorecards to the COR and the CO within one week of receipt of the scorecard and grade.

It is anticipated that the contractor will be evaluated along the following dimensions:

- Code Quality and Standards Adherence: Contractor code will be evaluated by Government teams and IV&V providers. Code will be evaluated against standards published by USCIS, including design standards and architecture. Automated code review tools will also be used to validate code quality.
- Business Satisfaction: Each feature completed by a contractor team will be evaluated by the Government Product Owner for that team, and possibly by SMEs assigned to the team. At each iteration review, the functionality will be evaluated by a wider audience of Government employees.
- Test Quality and Test Coverage: Test scripts and code will be treated as deliverables. These test scripts and code will be assessed for their quality and for the extent to which they test the appropriate functions. This evaluation will be performed by the IV&V test team or Government employees.
- Production Performance: The contractor will be evaluated on the performance of their code in production, its availability, response time, usability, accuracy and lack of defects.
- Collaboration: USCIS RFAD Contractor teams will operate within an ecosystem of federal and contractor staff, with multiple contractor teams working in parallel and with constant interaction with USCIS employees. The contractor will be graded based on their willingness, effort, and ability to work collaboratively.
- Productivity: Although measures such as velocity and story point completion cannot be used directly in an Agile process to measure performance, the Government will evaluate the value delivered and will also note any unproductive behavior.
- Process and Continuous Improvement: USCIS RFAD contractor teams will be assessed on the processes they implement, their conformance to USCIS processes, their conformance with Systems Engineering Life Cycle (SELC) and other required frameworks, and their use of retrospectives to continuously improve these processes.

Based on the tasks in Section 4 and this performance criteria, the contractor shall provide a draft Quality Assurance Surveillance Plan (QASP) following award. The government will review and coordinate with the contractor to develop a final version of the QASP to be utilized.

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 sensitive but unclassified information, and that the Contractor will adhere to the following.

SUITABILITY DETERMINATION

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

BACKGROUND INVESTIGATIONS

Contractor employees (to include applicants, temporaries, part-time and replacement employees) under the contract, needing access to sensitive but unclassified information shall undergo a position sensitivity analysis based on the duties each individual will perform on the contract as outlined in the 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.

To the extent the Position Designation Determination form reveals that the Contractor will not require access to sensitive but unclassified information or access to USCIS IT systems, OSI PSD may determine that preliminary security screening and or a complete background investigation is not required for performance on this contract.

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

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

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

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

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

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

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

CONTINUED ELIGIBILITY

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

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

In support of the overall USCIS mission, Contractor employees are required to complete one-time or annual DHS/USCIS mandatory trainings. The Contractor shall certify annually, but no later than

December 31st each year, or prior to any accelerated deadlines designated by USCIS, that required trainings have been completed. The certification of the completion of the trainings by all contractors shall be provided to both the COR and Contracting Officer.

- **USCIS Security Awareness Training** (required within 30 days of entry on duty for new contractors, and annually thereafter)
- **USCIS Integrity Training** (Annually)
- **DHS Insider Threat Training** (Annually)
- **DHS Continuity of Operations Awareness Training** (one-time training for contractors identified as providing an essential service)
- **Unauthorized Disclosure Training** (one time training for contractors who require access to USCIS information regardless if performance occurs within USCIS facilities or at a company owned and operated facility)
- **USCIS Fire Prevention and Safety Training** (one-time training for contractors working within USCIS facilities; contractor companies may substitute their 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 Corporate Security Officer. The individual will interface with OSI through the COR on all security matters, to include physical, personnel, and protection of all Government information and data accessed by the Contractor.

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

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

SECURITY PROGRAM BACKGROUND

The DHS has established a department wide IT security program based on the following Executive Orders (EO), public laws, and national policy:

- Public Law 107-296, Homeland Security Act of 2002.
- Federal Information Security Management Act (FISMA) of 2002, November 25, 2002.
- Public Law 104-106, Clinger-Cohen Act of 1996 [formerly, Information Technology Management Reform Act (ITMRA)], February 10, 1996.
- Privacy Act of 1974, As Amended. 5 United States Code (U.S.C.) 552a, Public Law 93-579, Washington, D.C., July 14, 1987.
- Executive Order 12829, *National Industrial Security Program*, January 6, 1993.
- Executive Order 12958, *Classified National Security Information*, as amended.
- Executive Order 12968, *Access to Classified Information,* August 2, 1995.
- Executive Order 13231, *Critical Infrastructure Protection in the Information Age*, October 16, 2001
- National Industrial Security Program Operating Manual (NISPOM), February 2001.
- DHS *Sensitive Systems Policy Publication 4300A* v2.1, July 26, 2004

- DHS *National Security Systems Policy Publication 4300B* v2.1, July 26, 2004
- Homeland Security Presidential Directive 7, *Critical Infrastructure Identification, Prioritization, and Protection*, December 17, 2003.
- Office of Management and Budget (OMB) Circular A-130, *Management of Federal*
- *Information Resources.*
- National Security Directive (NSD) 42, *National Policy for the Security of National Security Telecommunications and Information Systems* (U), July 5, 1990, CONFIDENTIAL.
- 5 Code of Federal Regulations (CFR) §2635, Office of Government Ethics, *Standards of Ethical Conduct for Employees of the Executive Branch.*
- DHS SCG OS-002 (IT), National Security IT Systems Certification & Accreditation, March 2004.
- Department of State 12 Foreign Affairs Manual (FAM) 600, *Information Security*
- *Technology*, June 22, 2000.
- Department of State 12 FAM 500, *Information Security*, October 1, 1999.
- Executive Order 12472, *Assignment of National Security and Emergency Preparedness Telecommunications Functions*, dated April 3, 1984.
- Presidential Decision Directive 67, *Enduring Constitutional Government and Continuity of Government Operations*, dated October 21, 1998.
- FEMA Federal Preparedness Circular 65, *Federal Executive Branch Continuity of Operations (COOP)*, dated July 26, 1999.
- FEMA Federal Preparedness Circular 66, *Test, Training and Exercise (TT&E) for Continuity of Operations (COOP)*, dated April 30, 2001.
- FEMA Federal Preparedness Circular 67, *Acquisition of Alternate Facilities for Continuity of Operations*, dated April 30, 2001.
- Title 36 Code of Federal Regulations 1236, Management of Vital Records, revised as of July 1, 2000.
- National Institute of Standards and Technology (NIST) Special Publications for computer security and FISMA compliance.

GENERAL

Due to the sensitive nature of USCIS information, the contractor is required to develop and maintain a comprehensive Computer and Telecommunications Security Program to address the integrity, confidentiality, and availability of sensitive but unclassified (SBU) information during collection, storage, transmission, and disposal. The contractor's security program shall adhere to the requirements set forth in the DHS Management Directive 4300 IT Systems Security Pub Volume 1 Part A and DHS Management Directive 4300 IT Systems Security Pub Volume I Part B. This shall include conformance with the DHS Sensitive Systems Handbook, DHS Management Directive 11042 Safeguarding Sensitive but Unclassified (For Official Use Only) Information and other DHS or USCIS guidelines and directives regarding information security requirements. The contractor shall establish a working relationship with the USCIS IT Security Office, headed by the Information Systems Security Program Manager (ISSM).

IT SYSTEMS SECURITY

In accordance with DHS Management Directive 4300.1 "Information Technology Systems Security", USCIS Contractors shall ensure that all employees with access to USCIS IT Systems are in compliance with the requirement of this Management Directive. Specifically, all contractor

employees with access to USCIS IT Systems meet the requirement for successfully completing the annual "Computer Security Awareness Training (CSAT)." All contractor employees are required to complete the training within 60-days from the date of entry on duty (EOD) and are required to complete the training yearly thereafter.
CSAT can be accessed at the following: http://otcd.uscis.dhs.gov/EDvantage.Default.asp or via remote access from a CD which can be obtained by contacting uscisitsecurity@dhs.gov.

IT SECURITY IN THE SYSTEMS DEVELOPMENT LIFE CYCLE (SDLC)

The USCIS SDLC Manual documents all system activities required for the development, operation, and disposition of IT security systems. Required systems analysis, deliverables, and security activities are identified in the SDLC manual by lifecycle phase. The contractor shall assist the appropriate USCIS ISSO with development and completion of all SDLC activities and deliverables contained in the SDLC. The SDLC is supplemented with information from DHS and USCIS Policies and procedures as well as the National Institute of Standards Special Procedures related to computer security and FISMA compliance. These activities include development of the following documents:

- *Sensitive System Security Plan (SSSP)*: This is the primary reference that describes system sensitivity, criticality, security controls, policies, and procedures. The SSSP shall be based upon the completion of the DHS FIPS 199 workbook to categorize the system of application and completion of the RMS Questionnaire. The SSSP shall be completed as part of the System or Release Definition Process in the SDLC and shall not be waived or tailored.
- *Privacy Impact Assessment (PIA) and System of Records Notification (SORN).* For each new development activity, each incremental system update, or system recertification, a PIA and SORN shall be evaluated. If the system (or modification) triggers a PIA the contractor shall support the development of PIA and SORN as required. The Privacy Act of 1974 requires the PIA and shall be part of the SDLC process performed at either System or Release Definition.
- *Contingency Plan (CP)*: This plan describes the steps to be taken to ensure that an automated system or facility can be recovered from service disruptions in the event of emergencies and/or disasters. The Contractor shall support annual contingency plan testing and shall provide a Contingency Plan Test Results Report.
- *Security Test and Evaluation (ST&E)*: This document evaluates each security control and countermeasure to verify operation in the manner intended. Test parameters are established based on results of the RA. An ST&E shall be conducted for each Major Application and each General Support System as part of the certification process. The Contractor shall support this process.
- *Risk Assessment (RA):* This document identifies threats and vulnerabilities, assesses the impacts of the threats, evaluates in-place countermeasures, and identifies additional countermeasures necessary to ensure an acceptable level of security. The RA shall be completed after completing the NIST 800-53 evaluation, Contingency Plan Testing, and the ST&E. Identified weakness shall be documented in a Plan of Action and Milestone (POA&M) in the USCIS Trusted Agent FISMA (TAF) tool. Each POA&M entry shall identify the cost of mitigating the weakness and the schedule for mitigating the weakness, as well as a POC for the mitigation efforts.
- *Certification and Accreditation (C&A):* This program establishes the extent to which a particular design and implementation of an automated system and the facilities housing that system meet a specified set of security requirements, based on the RA of security features

and other technical requirements (certification), and the management authorization and approval of a system to process sensitive but unclassified information (accreditation). As appropriate the Contractor shall be granted access to the USCIS TAF and Risk Management System (RMS) tools to support C&A and its annual assessment requirements. Annual assessment activities shall include completion of the NIST 800-26 Self-Assessment in TAF, annual review of user accounts, and annual review of the FIPS categorization. C&A status shall be reviewed for each incremental system update and a new full C&A process completed when a major system revision is anticipated.

SECURITY ASSURANCES

DHS Management Directives 4300 requires compliance with standards set forth by NIST, for evaluating computer systems used for processing SBU information. The Contractor shall ensure that requirements are allocated in the functional requirements and system design documents to security requirements are based on the DHS policy, NIST standards and applicable legislation and regulatory requirements. Systems shall offer the following visible security features:

- *User Identification and Authentication (I&A)* – I&A is the process of telling a system the identity of a subject (for example, a user) (*I*) and providing that the subject is who it claims to be (*A*). Systems shall be designed so that the identity of each user shall be established prior to authorizing system access, each system user shall have his/her own user ID and password, and each user is authenticated before access is permitted. All system and database administrative users shall have strong authentication, with passwords that shall conform to established DHS standards. All USCIS Identification and Authentication shall be done using the Password Issuance Control System (PICS) or its successor. Under no circumstances will Identification and Authentication be performed by other than the USCIS standard system in use at the time of a systems development.
- *Discretionary Access Control (DAC)* – DAC is a DHS access policy that restricts access to system objects (for example, files, directories, devices) based on the identity of the users and/or groups to which they belong. All system files shall be protected by a secondary access control measure.
- *Object Reuse* – Object Reuse is the reassignment to a subject (for example, user) of a medium that previously contained an object (for example, file). Systems that use memory to temporarily store user I&A information and any other SBU information shall be cleared before reallocation.
- *Audit* – DHS systems shall provide facilities for transaction auditing, which is the examination of a set of chronological records that provide evidence of system and user activity. Evidence of active review of audit logs shall be provided to the USCIS IT Security Office on a monthly basis, identifying all security findings including failed log in attempts, attempts to access restricted information, and password change activity.
- *Banner Pages* – DHS systems shall provide appropriate security banners at start up identifying the system or application as being a Government asset and subject to government laws and regulations. This requirement does not apply to public facing internet pages, but shall apply to intranet applications.

DATA SECURITY

SBU systems shall be protected from unauthorized access, modification, and denial of service. The Contractor shall ensure that all aspects of data security requirements (i.e., confidentiality, integrity, and availability) are included in the functional requirements and system design, and ensure that they meet the minimum requirements as set forth in the DHS Sensitive Systems Handbook and USCIS policies and procedures. These requirements include:

- *Integrity* – The computer systems used for processing SBU shall have data integrity controls to ensure that data is not modified (intentionally or unintentionally) or repudiated by either the sender or the receiver of the information. A risk analysis and vulnerability assessment shall be performed to determine what type of data integrity controls (e.g., cyclical redundancy checks, message authentication codes, security hash functions, and digital signatures, etc.) shall be used.
- *Confidentiality* – Controls shall be included to ensure that SBU information collected, stored, and transmitted by the system is protected against compromise. A risk analysis and vulnerability assessment shall be performed to determine if threats to the SBU exist. If it exists, data encryption shall be used to mitigate such threats.
- *Availability* – Controls shall be included to ensure that the system is continuously working and all services are fully available within a timeframe commensurate with the availability needs of the user community and the criticality of the information processed.
- *Data Labeling.* – The contractor shall ensure that documents and media are labeled consistent with the DHS *Sensitive Systems Handbook.*

Enterprise Architecture (EA) Compliance Language

This is a list of EA Architecture Compliance language agreed upon between Components and HQ DHS to be used in preparing SOW, PWS & SOO for IT acquisitions & services. The following Components (CBP, TSA & USCG) have their own customized version listed below that must be used. All other Components must use the DHS Enterprise Architecture Compliance language that follows:

DHS Enterprise Architecture Compliance

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

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

Capitalized Property, Plant and Equipment (PP&E) Assets Internal Use Software (IUS)

1. Background

The United States Citizenship and Immigration Services Management Directive No. 128-001, USCIS/Office of Information Technology has an ongoing requirement to report Internal Use Software (IUS) costs for the programs under their purview and assignment. This report is a monthly mandatory requirement, and must include all software releases with a cumulative cost of $500K or greater; bulk purchases of $1 Million, and a useful life of 2 years or more.

2. Requirement

Reporting: All applicable charges for application releases and/or development charges are tracked and reported; documented by each applicable release so that an OIT determination can be made if the asset meets IUS criteria. USCIS has determined that the best method for identifying IUS candidates is through monthly collection of contractor cost data for all releases in development, and will capitalize the cost of an IUS project if it is classified as a G-PP&E asset and meets the required criteria.

Definition: IUS is software that is purchased from commercial off-the-shelf (COTS) vendors or ready to use with little or no changes. Internal developed software is developed by employees of USCIS, including new software and existing or purchased software that is modified with or without a contractor's assistance. Contractor-developed software is used to design, program, install, and implement, including new software and the modification of existing or purchased software and related systems, solely to meet the entity's internal or operational needs.

Invoicing and Reporting: The contractor shall identify, capture, log, track and report the costs of IUS associated with each specific release. IUS Software is typically release centric and includes the application and operating system programs, procedures, rules, and any associated documentation pertaining to the operation of a computer system or program.

The contractor shall, after OIT's determination on whether or not the release meets the capitalization criteria, support OIT's reporting of costs incurred for the project or release, as required. The contractor shall provide the nature and cost of work completed within the relevant period. Costs considered part of IUS activities include systems administration, systems engineering, and program management. The Contractor shall provide the total cost, itemized by release and include the total sum of all applicable IUS activities. At the contractor's discretion, this information may be submitted, either as an attachment or as an itemized line item within the monthly invoices, as outlined in *Table 2: Deliverables Schedule.* For information purposes, the following activities within the development lifecycle have been identified as IUS reportable costs by the USCIS Management Directive No. 128-001:

1) Design: System Design: Design System, Update System Test Plan, Update Security Test Plan, Update Project Plan, Update Business Case, Conduct Critical Design Review and Issue Memo.

2) Programming/Construction: Establish Development Environment, Create or Modify Programs, Conduct Unit & Integration Testing, Develop Operator's Manual, Update

Project Plan, Update Business Case, Migration Turnover/Test Readiness Review, Prepare Turnover Package, Develop Test Plans, Migration Turnover/Issue Test Readiness Memo

3) Testing

    a. Acceptance Testing: Develop Security Test Report, Issue Security Certification, Develop System Documentation, Conduct User Acceptance Testing, Update Project Plan, Update Business Case, Conduct Production Readiness Review, Develop Implementation Plan, Issue Production Readiness Review Memo.

    b. Coding

    c. Installation to hardware

    d. Testing, including parallel processing phase

4) Implementation Activities: Implementation/Transition: Security Accreditation (initial system accreditation only), Issue Implementation Notice, Parallel Operations, Update Project Plans, Update Business Case, Conduct Operational Readiness Review, Issue Operational Readiness Memo.

5) In addition, these cost shall contain, if not already itemized in the attachment (PER) or the invoice, the following additional costs information: Full cost (i.e., direct and indirect costs) relating to software development phase; Travel expenses by employees/contractor directly associated with developing software; Documentation Manuals; COTS purchases.

Attachment 5 - RFAD 70SBUR18F00000697

Section 508 Compliance

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 information and communications technology (ICT), it shall be accessible to people with disabilities. Federal employees and members of the public who have disabilities must have access to and use of information and data that is comparable to Federal employees and members of the public without disabilities. All products, platforms, and services delivered as part of this work statement that are by definition ICT or contain ICT shall conform to the Revised 508 Standards, which are located at 36 C.F.R. § Appendices A, C, and D, and available at https://www.gpo.gov/fdsys/pkg/CFR-2017-title36-vol3/pdf/CFR-2017-title36-vol3-part1194.pdf.

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

Section 508 Applicable EIT Accessibility Standards

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

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

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

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

Section 508 Applicable Exceptions

Exceptions for this work statement have been determined by DHS and only the exceptions described herein may be applied. Any request for additional exceptions shall be sent to the 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. Agencies cannot claim a product as a whole is not commercially available because no product in the marketplace meets all the standards. If products are commercially available that meets some but not all of the standards, the agency must procure the product that best meets the standards. When applying this standard, all procurements of EIT shall have documentation of market research that identify a list of products or services that first meet the agency business needs, and from that list of products or services, an analysis that the selected product met more of the accessibility requirements than the non-selected products as required by FAR 39.2. Any selection of a product or service that meets less accessibility standards due to a significant difficulty or expense shall only be permitted under an undue burden claim and requires authorization from the DHS Office of Accessible Systems and Technology (OAST) in accordance with DHS MD 4010.2.

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

[redacted]

[redacted]