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

1. REQUISITION NUMBER	PAGE	OF
OIT196025A	1	52

2. CONTRACT NO.	3. AWARD/ EFFECTIVE DATE	4. ORDER NUMBER	5. SOLICITATION NUMBER	6. SOLICITATION ISSUE DATE
GS00Q17GWD2163		70SBUR19F00000188	70SBUR19R00000041	04/16/2019

7. FOR SOLICITATION INFORMATION CALL:	a. NAME	b. TELEPHONE NUMBER (No collect calls)	8. OFFER DUE DATE/LOCAL TIME
	HOLLIE WALSH	[redacted]	

9. ISSUED BY	CODE	10. THIS ACQUISITION IS
USCIS Contracting Office Department of Homeland Security 70 Kimball Avenue South Burlington VT 05403	CIS	☐ UNRESTRICTED OR ☒ SET ASIDE: 100.00 % FOR: ☐ SMALL BUSINESS ☐ HUBZONE SMALL BUSINESS ☐ SERVICE-DISABLED VETERAN-OWNED SMALL BUSINESS ☐ WOMEN-OWNED SMALL BUSINESS (WOSB) ELIGIBLE UNDER THE WOMEN-OWNED SMALL BUSINESS PROGRAM ☐ EDWOSB ☒ 8(A) NAICS: 541511 SIZE STANDARD: $27.5

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

15. DELIVER TO	CODE	16. ADMINISTERED BY	CODE
Department of Homeland Security Citizenship & Immigration Services CIS Contracting Office 70 Kimball Avenue South Burlington VT 05403	CIS	USCIS Contracting Office Department of Homeland Security 70 Kimball Avenue South Burlington VT 05403	CIS

17a. CONTRACTOR/ OFFEROR	CODE	FACILITY CODE	18a. PAYMENT WILL BE MADE BY	CODE
I-LINK SOLUTIONS INC 1760 RESTON PARKWAY SUITE 214 RESTON VA 201903429 TELEPHONE NO.	9620053230000		See Invoicing Instructions	WEBVIEW

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

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: 962005323+0000 --- Integration Architecture Services (IAS) --- Attachments 1-5 (attached) are incorporated into this task order. The terms and conditions of the contractor's 8(a) Stars II contract apply. *(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: _____ OFFER DATED _____. 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)*	31c. DATE SIGNED
		Kiley Leahy	4/30/19

AUTHORIZED FOR LOCAL REPRODUCTION
PREVIOUS EDITION IS NOT USABLE

STANDARD FORM 1449 (REV. 2/2012)
Prescribed by GSA - FAR (48 CFR) 53.212

19. ITEM NO.	20. SCHEDULE OF SUPPLIES/SERVICES	21. QUANTITY	22. UNIT	23. UNIT PRICE	24. AMOUNT
	[redacted]				
	AAP Number: 2019045005				
0001	DevSecOps Team (PSC D302) Firm-Fixed Price	12	MO	[redacted]	[redacted]
	Delivery: 60 Days After Award Accounting Info: ITENTSR ESB EP 20-05-00-000 23-20-0600-00-00-00-00 GE-25-86-00 000000 Funded: [redacted] Accounting Info: ITENTSR PIO EP 20-05-00-000 23-20-0600-00-00-00-00 GE-25-86-00 000000 Funded: [redacted] Accounting Info: ITENTSR PTO EP 20-05-00-000 23-20-0600-00-00-00-00 GE-25-86-00 000000 Funded: [redacted] Accounting Info: EPROC00 000 EX 20-01-00-000 07-00-0000-00-00-00-00 GE-25-88-00 000000 Funded: [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	34. VOUCHER NUMBER	35. AMOUNT VERIFIED CORRECT FOR	36. PAYMENT	37. CHECK NUMBER
☐ PARTIAL ☐ FINAL			☐ COMPLETE ☐ PARTIAL ☐ FINAL	

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

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

STANDARD FORM 1449 (REV. 2/2012) BACK

NAME OF OFFEROR OR CONTRACTOR
I-LINK SOLUTIONS INC

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
1001	DevSecOps Team (PSC D302) Firm-Fixed Price Amount: [redacted] Anticipated Exercise Date: The total amount of award: [redacted]. The obligation for this award is shown in box 26.	12	MO	[redacted]	0.00

Part II—Task Order Clauses

Federal Acquisition Regulation (FAR) clauses incorporated by reference

52.203-19 Prohibition on Requiring Certain Internal Confidentiality Agreements or Statements (Jan 2017)

52.209-10 Prohibition on Contracting With Inverted Domestic Corporations (Nov 2015)

52.245-1 Government Property (Jan 2017)

Federal Acquisition Regulation (FAR) clauses incorporated in full text

52.203-99 Prohibition on Contracting With Entities That Require Certain Internal Confidentiality Agreements (DEVIATION) (Jul 2016)

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

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

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

(d) In accordance with Section 743 of Division E, Title VII, of the Consolidated and Further Continuing Appropriations Act, 2015, (Pub. L. 113-235) use of funds appropriated (or otherwise made available) under that or any other Act may be prohibited, if the government determines that the contractor is not in compliance with the provisions of this clause.

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

(f) The government may seek any available remedies in the event the contractor fails to comply with the provisions of this clause.

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

(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 24 months.

(End of clause)

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)

52.252-4 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 52.203-99. Prohibition On Contracting With Entities That Require Certain Internal Confidentiality Agreements 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

3052.203-70 Instructions for Contractor Disclosure 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.

(g) Before receiving access to IT resources under this contract the individual must receive a security briefing, which the Contracting Officer's Technical Representative (COTR) will arrange, and complete any nondisclosure agreement furnished by DHS.

(h) The Contractor shall have access only to those areas of DHS information technology resources explicitly stated in this contract or approved by the COTR in writing as necessary for performance of the work under this contract. Any attempts by Contractor personnel to gain access to any information technology resources not expressly authorized by the statement of work, other terms and conditions in this contract, or as approved in writing by the COTR, is strictly prohibited. In the event of violation of this provision, DHS will take appropriate actions with regard to the contract and the individual(s) involved.

(i) Contractor access to DHS networks from a remote location is a temporary privilege for mutual convenience while the Contractor performs business for the DHS Component. It is not a right, a guarantee of access, a condition of the contract, or Government Furnished Equipment (GFE).

(j) Contractor access will be terminated for unauthorized use. The Contractor agrees to hold and save DHS harmless from any unauthorized use and agrees not to request additional time or money under the contract for any delays resulting from unauthorized use or access.

(k) Non-U.S. citizens shall not be authorized to access or assist in the development, operation, management or maintenance of Department IT systems under the contract, unless a waiver has

been granted by the Head of the Component or designee, with the concurrence of both the Department's Chief Security Officer (CSO) and the Chief Information Officer (CIO) or their designees. Within DHS Headquarters, the waiver may be granted only with the approval of both the CSO and the CIO or their designees. In order for a waiver to be granted:

(1) There must be a compelling reason for using this individual as opposed to a U. S. citizen; and

(2) The waiver must be in the best interest of the Government.

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

(End of clause)

3052.215-70 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.

The Key Personnel or Facilities under this Contract: Program Manager

(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 Task Order Requirements

II-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

(e) On CLIN 0001, if there is rework that needs to be completed on this CLIN, the invoice shall indicate the rate (less any profit).

II-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.

II-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.

II-4. KEY PERSONNEL

For the purposes of the contract clause at HSAR 3052.215-70, Key Personnel or Facilities, the Program Manager shall be Key Personnel on this task order and is listed in Section 7 in the Performance Work Statement (PWS). The Program Manager submitted by a contractor to fill a key person billet shall meet required standards per Section 7 of the PWS.

II-5. NOTICE TO PROCEED (NTP)

(a) Performance of the work requires unescorted access to government facilities or automated systems, and/or access to sensitive but unclassified information. The Security Requirements in section II-8 applies.

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

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

(d) This task order does not provide for direct payment to the contractor for EOD efforts. Work for which direct payment is not provided is a subsidiary obligation of the contractor. The contracting officer will issue a notice to proceed (NTP) at least one day before full performance is to begin.

(e) The government intends for performance to begin no later than **60 days** after task order award (allowing up to 60 days for the EOD period). The NTP will be granted when a minimum of two (2) personnel have EOD'd.

II-6. CONSENT TO SUBCONTRACT

For the purposes of the contract clause at FAR 52.244-2, Subcontracts, the fill-in for paragraph (d) is "ALL."

II-7. EXPECTATION OF CONTRACTOR PERSONNEL

The government expects competent, productive, qualified IT professionals to be assigned to the DevSecOps Team. The contracting officer may, by written notice to the contractor, require the

contractor to remove any employee that is not found to be competent, productive, or a qualified IT professional.

II-8. SECURITY REQUIREMENTS – Security Clause 5 (Oct 2018)

GENERAL

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

SUITABILITY DETERMINATION

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

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

BACKGROUND INVESTIGATIONS

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

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

Completed packages must be submitted to OSI PSD for prospective Contractor employees no less than 30 days before the starting date of the contract or 30 days prior to EOD of any employees, whether a

replacement, addition, subcontractor employee, or vendor. The Contractor shall follow guidelines for package submission as set forth by OSI PSD. A complete package will include the following forms, in conjunction with security questionnaire submission of the SF-85P, "Security Questionnaire for Public Trust Positions" via e-QIP:
1. DHS Form 11000-6, "Conditional Access to Sensitive But Unclassified Information Non-Disclosure Agreement"

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

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

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

5. USCIS Continuation Page to DHS Form 11000-25

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

7. Foreign National Relatives or Associates Statement

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

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

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

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

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

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

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

- **USCIS Security Awareness Training** (required within 30 days of entry on 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)
- **Computer Security Awareness Training** (if contractor requires access to USCIS IT systems, training must be completed within 60 days of entry on duty for new contractors, and annually thereafter)

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

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

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

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

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

Contractor employees who do not have a PIV card must schedule an appointment to have one issued.
To schedule an appointment:
http://ecn.uscis.dhs.gov/team/mgmt/Offices/osi/FSD/HSPD12/PIV/default.aspx
Contractors who are unable to access the hyperlink above shall contact the Contracting Officer's Representative (COR) for assistance.
Contractor employees who do not have a PIV card will need to be escorted at all times by a government employee while at a USCIS facility and will not be allowed access to USCIS IT systems.
A contractor employee required to have a PIV card shall:
• Properly display the PIV card above the waist and below the neck with the photo facing 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.

II-9. 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.

Part III—List of Attachments

Attachment #	Document Title	Pages
1	[redacted]	19
2	[redacted]	1
3	[redacted]	2
4	[redacted]	3
5	[redacted]	1

PERFORMANCE WORK STATEMENT

Integration and Architecture Services (IAS)

1. OVERVIEW

The U.S. Citizenship and Immigration Services (USCIS) [redacted] requires [redacted] Through the performance of this contract, USCIS will target specific modernization challenges of the USCIS enterprise integration layer that will rapidly deploy releases to take advantage of newly available Cloud tools along with pre-existing tools already deployed and adopted by USCIS. The objective of this contract is to utilize US digital service techniques to identify and solve core needs of Development, Security and Operations (DevSecOps) teams. [redacted] In order to achieve this objective, the contractor must maintain, update and execute a framework for DevSecOps, usability research, and agile implementation.

2. BACKGROUND

Today, USCIS provides benefits and services to people via paper-based processing of immigration forms. Paper-based processing creates significant business and technology challenges, as it limits USCIS' ability to efficiently address complex and evolving immigration needs. As an agency, USCIS faces increasing costs associated with handling the paper-based forms via mail, along with a number of data integrity challenges, from manual data entry errors to lack of real-time access to mission critical data.

USCIS is currently transforming its services culture from paper-based to digital; however, there are still significant challenges to overcome to align with digital transformation best practices and development of modernized services. In addition, there has been a rapid increase in industry innovation coming from [redacted] o bridge the gap between the wealth of experience that industry brings and USCIS' capacity to adopt emerging capabilities, the need exists to accelerate the modernization of the integration infrastructure layer.

3. SCOPE

The contractor shall support the USCIS mission to achieve end-to-end digital workflow processing, to include the ingestion of all paper-based correspondence, such as applications and evidence through adjudication, decision making, and communication with applicants, to

create digital immigration records at the point of receipt that serve as the official record throughout the immigration lifecycle.

The contractor shall provide this support through DevSecOps personnel that focus on development, IT operations and security. The team shall work collaboratively with other USCIS Agile teams and step outside the traditional channels, embracing automation and orchestration.

4. TASKS

The resulting contract will be considered successful when the following outputs have been delivered:

Workstream 1 – ESB Modernization

- Description: [redacted].
- Objectives:
  - Reverse engineer the existing [redacted] to determine the requirement
  - [redacted]
  - Build and deploy enterprise microservices that can be reused and repurposed
  - Conduct [redacted] (Continuous Integration/ Continuous Delivery) [redacted]
  - Document the new architecture and test plans
  - Add and update monitoring capability

- Path Forward:
  - Deliver staged services to production.
  - Conduct testing with partner systems to verify interoperability
  - Provide Operations and Maintenance (O&M) on the production deliveries
  - Develop a Concept of Operations (CONOPS) and all required documentation for each of the production deliveries

Workstream 2 – Integration Infrastructure Support

- Description: Enterprise tool training and adoption, Authority to Operate (ATO) and related efforts, as well as support for other USCIS development teams adopting modernized architecture and microservices.
- Objectives:
  - Provide training support to USCIS on enterprise tools, such as [redacted]
  - Provide assistance with infrastructure components, such as [redacted]

- Deliver Information [redacted] support for the Enterprise Integration Services security posture and [redacted]
- Provide reusable services for the enterprise such as [redacted]

- Path Forward:
  - [redacted]
  - Update Privacy Impact Assessment (PIA) for Enterprise Integration Services modules that contain PII
  - Lead governance on Kafka topic creation
  - Get Enterprise Integration Services to Ongoing Authorization (OA) status on production modules

Workstream 3 – [redacted]

- Description: Provides support for the tasks identified below
- Objectives:
  - [redacted]
  - [redacted]
  - [redacted]
  - Internal/External API product development for third parties for data exchange
- Path Forward:
  - Deliver increments of Enterprise Integration Payment Service as requirements expand
  - Update and enhance [redacted] and continue the refresh of datasets as required by business
  - Enhance and deploy PDF Generation or [redacted] rendering Service in iterations as business requirements are communicated
  - Deliver, upgrade, enhance and maintain external API products in the form of digital benefits, payments and communications.

5. TECHNOLOGY AND TECHNIQUES

5.1 Methodology

The Contractor's support and solutions shall align with the U.S. Digital Services Playbook https://playbook.cio.gov and the Open Practice Library https://openpracticelibrary.com/.

The Contractor shall:

- Be familiar with the concepts in each play/practice and implement them in its approaches and support for USCIS.
- Participate in USCIS's Agile methodologies and related ceremonies (e.g. backlog grooming, sprint planning, daily stand-ups, sprint review, sprint retrospective, scrum of scrums).
- Be responsible for the activities associated with design, development, configuration, customization and deployment of solutions.
- Once solutions are deployed, provide production support and enhancements as required.

The Contractor shall adhere to modern digital services that use [redacted] The Contractor shall deliver secure and tested mobile and web designs and applications using automated testing frameworks that utilize services, microservices and containers.

The Contractor shall work closely with the Government IT program managers and electronic processing business owners to conduct user research, create, groom, develop, design, prioritize and test user stories that will serve as the foundation for the development work. The product management team from electronic processing and integration architecture provides guidance on product vision, business requirements and priority of work as well as validation that user stories meet the acceptance criteria for each story. The OIT program managers provide technical and contract oversight. The integration architecture OIT program managers will impart process, workflow and operational procedures.

5.2 Agile Development

[redacted] The Contractor shall deliver high quality, production-ready functionality in an incremental fashion using Agile development practices and methods. The Contractor [redacted] which may include but are not limited to grooming, review, planning, and retrospective. The Contractor shall deliver all requested documents including, but not limited to, lifecycle management gate review documents, status reports, metrics reports, process flows, presentations, minutes, flow charts, designs, trip reports and research plans. [redacted] The Contractor shall update and maintain a central document repository so that information remains relevant and easy to locate. This archive of information is crucial to the management of the program.

5.3 DevSecOps

DevSecOps is an integral part of supporting USCIS. The Contractor shall support the [redacted] and shall monitor and maintain multiple environments with CI/CD pipelines that utilize automated builds, automated tests and static analysis. The Contractor shall support proactive monitoring and analysis to ensure that the systems and its interfaces are available and functioning properly. The Contractor shall support daily automated performance testing to ensure that the responsiveness and stability of the application, and the systems that are integrated with it, are maintained. The contractor shall support working agreements and contract testing with all interface partners. [redacted] rather they [redacted] The Contractor shall update and assist with updating the required security documentation for the project, including but not limited to the System Security Plan.

5.4 Documentation

The Contractor shall design, develop, deploy, and maintain solutions under the governance of the USCIS Agile development methodologies, to include preparation and delivery of the USCIS required system documentation. If USCIS issues updated version(s) of documents and development methodologies, then the Contractor shall adhere to the most recently published updated version so that all new products and services shall follow the format, content and direction specified in the most recently published updated version of the documents as applicable. The Contractor shall provide support in creating the necessary documentation for Release Planning Reviews (RPR) and Release Readiness Reviews (RRR), where the program is reviewed and certified by the USCIS security, quality assurance (QA), 508 Compliance teams, OIT Program Manager, and Chief Information Officer (CIO). Examples of documentation include, but are not limited to, the Interface Control Agreements, System Design Document, Pipeline Design Document, Test Plan, and System Workload Analysis Document.

The Contractor shall prepare documentation for and attend a combined Post Implementation Review and a Release Planning Review with the CIO and other Government leadership staff from OIT. At this meeting, which occurs every six months, the Contractor shall provide retrospective details on the previous six month release cycle and shall also outline the roadmap for the upcoming six month release cycle using document templates and guidance from the USCIS Quality Assurance team. These templates outline the capabilities and constraints, system integrations, system design, and pipeline design among other things. The Contractor shall work with the USCIS Federal Program leads to update these documents. The meeting is an in person discussion at USCIS HQ, 111 Massachusetts Avenue NW Washington DC.

The Contractor shall produce and deliver documentation that will become the property of USCIS. This documentation shall include technical documentation, system diagrams, code repository information, user guides and any and all documents that support transition of work to other Contractors or Government personnel.

5.5 Current Technical Stack & Tools

Table below is the current tool suite that the contractor is expected use unless directed specifically by USCIS's CIO and or CTO. This tool suite is subject to change.

Name	Version	Manufacturer	Function
ActiveMQ	5.14.0	Apache	Messaging
Adobe Livecycle	11.0.0	Adobe	Adobe Livecycle
Amazon Web Services	Latest	Amazon	Cloud computing services
AngularJS	1.2.	AngularJS	Javascript Framework
Ansible	v2.3.1.0-1	OSS GNU	Open Source simple IT automation platform
Apigee	14.17.05	Google	CLOUD NATIVE API Management Platform for ensuring security, visibility, and performance across the entire API landscape (pending for procurement).
Apache Portable Runtime (APR)	1.5.1	Apache Software Foundation	Apache performance support for Apache Tomcat
Apache Tomcat Native	1.1.33	Apache Software Foundation	Required for Apache Portable Runtime
Beyond Compare	4.2.2	Scooter Software	Developer tool for comparing files and directories
Chef	11.4	Opscode	Open source software deployment

Name	Version	Manufacturer	Function
Cloudbees Jenkins	2.7.19.1	Cloudbees	Commercial continuous integration server to build declarative pipelines.
Confluence	5.10.2	Atlassian	Documentation Wiki
Docker	1.12.6	Docker Inc	Software containerization and deployment
Eclipse	Neon	Eclipse	IDE for software development
Fortify	16.1	HP	Static Code Analysis
GitHub Enterprise	2.9	GitHub	Hosted code management
GitRob	1.1.12	MIT	Open Source Reconnaissance tool for GitHub
Gradle	2.13	Gradle.org	Open source build automation tool
Hibernate	4	Jboss	Open source object / relational mapping library for Java
Hygieia	2.0.5	CapitalOne	Hygieia (Also called "devops-dashboard") is a single, configurable, easy to use dashboard to visualize near real-time status of the entire delivery pipeline, JIRA integration & status on your user stories, Issue, defects and Bugs tracking.
Java	1.8	Oracle	Language for software development

Name	Version	Manufacturer	Function
Java Development Kit	1.7.25	Oracle Software	Required for Apache Tomcat application deployments
Jboss Application Server	7.0.2	Jboss	Open source application server
Jboss Rules Engine	5	Jboss	Open source rules engine
Jenkins	2.66	Jenkins CI	Open source continuous integration server
Jira	7.1.19	Atlassian	COTS ALM tool
Junit	LATEST	Apache	Unit testing
JNISTPack	1.7.1	AWARE	Allows creating, reading and updating of NIST files
KeePass	2.36	KeePass	Password Management tool
Kong	0.10.3	Mashape	API Gateway Layer Software
Liquibase	2.0.5	Liquibase.org	Open source database source code control
MongoDB	3.4	10gen, Inc	Open source document oriented database system
Nexus	3.3.0-01	Sonatype	Open source repository manager
Obsidian	4.3.0	Carfey	Scheduler
Openshift	3.4.1.18	RedHat	Container Platform/Orchestration tool
Oracle Database	11gR2	Oracle	Commercial database

Name	Version	Manufacturer	Function
OWASP	LATEST	Creative Commons	Open Web application Security Project
PostgreSQL	9.6.2	OpenSource	Permanent data source
MySQL Workbench	6.2.5.0	Oracle	Developer DBA tool (community edition)
Selenium	LATEST		Browser testing in Firefox
Slack	LATEST SAAS	Slack	Collaboration tool
SonarQube	6.4	Maintained by SonarSource	OSS Static Code Analysis
Spring Framework	3.1.0e3.8	SpringSource.org	Open source Java framework
Tableau	Latest	Tableau	Business intelligence & data visualization
Terraform	0.9.8	HashiCorp	Infrastructure as Code aid
Twistlock	2.0	Twistlock	Container Vulnerability Scanning
WebInspect	17.1	Hewlett Packard	Dynamic security testing application
Apache Camel	2.21.0		
Spring Boot	1.4.1	SpringSource.org	Spring Boot is a lightweight framework to provide a set of tools for quickly building Spring applications that are easy to configure.

Name	Version	Manufacturer	Function
Cirrus Framework	2.7.2	ConSol Software	Open source framework that provides a test automation framework for enterprise integration testing.
FUSE	6.3.0	Red Hat	Red Hat JBoss Fuse is a lightweight, flexible integration platform that enables rapid integration across the extended enterprise—on premise or in the cloud.
Kafka	2.12	Apache	Kafka is used for building real-time data pipelines and streaming apps.
Dynamo DB		AWS service	Fast and flexible NoSQL database service for all applications that need consistent, single-digit millisecond latency at any scale.
Splunk		Splunk	Splunk is a software platform to search, analyze and visualize the machine-generated data gathered from the websites, applications, sensors, devices etc. which make up your IT infrastructure and business.
SOAPUI	5.3	SMARTBEAR	Testing tool (open source)
SQL Developer	17.4.0.355	Oracle	Developer DBA tool (open source)

Name	Version	Manufacturer	Function
ZAP Proxy		Zapproxy	The OWASP Zed Attack Proxy (ZAP) is one of the world's most popular free security tools
SMTP			USCIS SMTP for sending notifications.
SQL Server Management Studio			Database studio to connect to SQL Server
TIBCO Business Events Decision Manager	5.1.1	TIBCO	Rules Engine
TIBCO Business Events Event Stream Processing	5.1.1	TIBCO	Rules Engine
Oracle Database server	11g RAC (11.2.0.1.0)	Oracle	DB
Oracle Client Interface	10.2.0.4	Oracle	DB
Apache Tomcat	7.0.59	Apache	Web-server
Apache HTTP Server	2.2.31	Apache	Reverse Proxy
Microsoft Windows Server 2008 R2 Enterprise	Microsoft Windows Server 2008 R2 SP1	Microsoft	OS
Solaris 10	10 10/09	Oracle	OS

Name	Version	Manufacturer	Function
Oracle JDBC Drivers	11G R2 – 11.2.0.1.0 10G – 10.2.0.4	Oracle	DB
Hibernate Core for Java	3.3.5	Open	DB
TIBCO Business Events Standard	5.1.1	TIBCO	Rules Engine
TIBCO Business Events Data Modeling	5.1.1	TIBCO	Rules Engine
TIBCO Runtime Agent	5.7.0 & 5.8.0	TIBCO	Back-end for TIBCO
TIBCO BusinessWorks Service Engine	5.9 & 5.11	TIBCO	Services
TIBCO ActiveMatrix – BusinessWorks	5.9 & 5.11	TIBCO	Services
TIBCO Enterprise Message Service (EMS)	8.3.0	TIBCO	JMS/Messaging
Microsoft SQL Server	TBD	Microsoft	DB
TIBCO Business Works Process Monitoring (BWPM)	TBD	TIBCO	Monitoring
TIBCO Designer	5.7.0 & 5.8.0	TIBCO	IDE for TIBCO
TIBCO Administrator – Enterprise Edition	5.9.0	TIBCO	Application Domain

Name	Version	Manufacturer	Function
TIBCO BusinessWorks Process Manager	3.2.0.4	TIBCO Software	Development tool to support BW/BE engine debugging
TIBCO BW JSON/REST plugin	2.0.0	TIBCO Software	Plugin to support JSON / REST for TIBCO BusinessWorks
TIBCO Database Driver Supplement	2.0.6	TIBCO Software	Provides DB drivers to allow Database access
TIBCO Rendezvous	8.4.2	TIBCO Software	TIBCO Domain Communications Daemon
TIBCO Spotfire Server	7.0.1	TIBCO Software	Analytics platform
TIBCO Spotfire Web Player	7.0.1	TIBCO Software	Analytics platform
Foglight Agent Manager for windows (64 bit)	5.8.5.8	Quest	Client application that manages Foglight agents installed on monitored hosts
Foglight Management Server windows (64 bit)	5.7.5.8	Quest	The Management Server receives information from agents, stores and processes data, and makes it available in the browser interface.
Foglight TIBCO cartridge	5.7.5.17	Quest	Foglight extended their Catridge functionality to monitor the TIBCO suite of products such as TIBCO ActiveMatrix BusinessWorks, Enterprise Message Service(EMS), and ActiveMatrix BusinessEvents
Foglight Cartridge for Infrastructure	5.8.5.8	Quest	Cartridges extend the functionality of Foglight and are

Name	Version	Manufacturer	Function
			installed on the Management Server

6. TEAM STRUCTURE

The contractor shall provide [redacted]. The contractor team's work shall conform to the architecture and design provided by USCIS and the agile processes set up by USCIS but managed by the team. The team must have all of the skills necessary to perform the tasks indicated in Section 4. It is important that the team as a whole has the skills necessary for development, operations, security, and test, but that does not mean that specific team members must be designated as testers, coders, etc. Most team members should have more than one skill. All personnel shall be mid-level to senior level labor categories. The contractor shall determine the labor mix for the team to provide the best overall solution to the government.

7. KEY PERSONNEL – [redacted]

- [redacted]

8. PLACE OF PERFORMANCE

[redacted]

[redacted]

9. TRAVEL

Travel is not anticipated for this requirement.

10. GOVERNMENT FURNISHED PROPERTY (GFP) (Reference FAR 52.245-1 Clause)

USCIS will provide contractor staff with GFP laptops. No personal or company owned storage devices, (thumb drives, DVDs, or CDs) will 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.

11. GOVERNMENT FURNISHED INFORMATION & SUPPORT

USCIS will grant access to the tools and software that is required to build and maintain an Office of Investigations Case Management application. For example, USCIS will provide access to the GitHub Enterprise code repositories and Jira/Confluence. All code will be located in the USCIS instance of GitHub Enterprise and is the property of USCIS. The USCIS Federal product managers and program managers will work closely with the contractor team to provide oversight and guidance to achieve the goals of the program.

12. DELIVERABLES

The contractor shall provide deliverables to the IT Program Manager and COR. Specific acceptance criteria will be identified with each user story. These deliverables are consistent with Agile methods and principles and vary based on team agreements and structure, scrum vs. Kanban. The contractor is encouraged to suggest alternative Agile methods and sprint durations if those suggested changes are intended to improve team communication, velocity, quality and speed of delivery to production.

SECTION	DELIVERABLE	INTERVAL	DESCRIPTION
4 & 5.2	Daily Stand Up	[redacted]	Discuss daily progress of the sprint, blockers etc.
4 & 5.2	Sprint Review	[redacted]	Demonstrate work that was completed in the sprint; explain work that was not able to be completed.

4 & 5.2	Burn Up Charts	[redacted]	Explain status of team progress against the scope of work.
4 & 5.2	Sprint Retrospective	[redacted]	Discuss the sprint, blockers, what went well etc. and use this info to continue to improve performance.
4 & 5.2	Sprint Planning	[redacted]	Establish sprint goals, plan and prioritize the work to be accomplished in the upcoming sprint including stretch goals.
4 & 5.2	Backlog Grooming	[redacted]	Groom and prioritize upcoming work and include dependencies.
4 & 5.2	Team Lead Check In	[redacted]	Discuss the progress of the overall program, Government's level of satisfaction with the contractor and any issues that need to be addressed. Plan for upcoming meetings or activities, discuss personnel changes.
4 & 5.2	Release Planning Review and Post Implementation Review Documentation	[redacted]	Update documentation Attend the RPR/PIR meeting.
4 & 5.2	Jira Confluence Wiki	[redacted]	Update project documents on the Jira Confluence Wiki on daily basis.
9	GFP Inventory	[redacted]	Excel

	(must contain CIS ID number, location, name of contactor holding equipment, date)		
Security Clause 5	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.
Solicitation Section II-3	Redacted copy of the executed task order including all attachments suitable for public posting under the provisions of the Freedom of Information Act (FOIA)	[redacted]	Email to foiaerr.nrc@uscis.dhs.gov with a courtesy copy to the CO.

13. PERFORMANCE MEASURES

Performance measures are gathered through tools and a CI/CD pipeline that calculates code and test coverage automatically.

Code Quality

Objective: Provide evidence that Code is maintained and improved. This applies to all custom code baseline inherited and newly developed:

[redacted]

Test Quality and Test Coverage
Objective: Provide evidence that test coverage meets the program policy for microservices, increase automated testing and test quality overtime.

[redacted]

System Stability
Objective: The system has high reliability, availability, and serviceability. Attention must be focused on the robustness of the system in the face of errors, the ability to be used as development proceeds, and the ability to quickly detect and correct latent problems:

[redacted]

Productivity
Objective: Provide evidence that there is focus on continuous productivity improvement. Provide evidence that the team is producing more of the right results. Engineering and development practices utilize the DevSecOps delivery models and tool consistently.

1. Teams provide evidence that they worked to reduce cycle time for their deliverables during the sprints. Reduce the latency between initiation of new work and delivery to production in order to enhance capability delivery to users. Cycle time – days between the start of work and deployment of work. Lead time -- days between initial request and deployment of work.
2. Teams shall capture the number of applicable orchestration processes, translation process and workflows identified vs. actually automated Survey assessment of development environment setup and access to development team percent of reported defects against a system/product.

Continuous Improvement:

Objective: Re-engineer where needed, eliminate duplicate lines of code, improve code hygiene, and show work in a self-assessment as needed.

1. Team provides a success flag for work that extends past 1 month (i.e. if work will not be completed in 1 month, define the success criteria / success flag for the 15 day evaluation period). Integration and Architecture Service contractor team will be assessed on the processes they implement, their alignment with USCIS processes and other required frameworks, and their use of retrospectives to continuously improve these processes.
2. [redacted]

14. Acceptance Criteria for Section 508 Requirements

1. Before accepting items that contain Information and Communications Technology (ICT) that are developed, modified, or configured according to this contract, the government reserves the right to require the contractor to provide the following:

    - Accessibility test results based on the required test methods.
    - Documentation of features provided to help achieve accessibility and usability for people with disabilities.
    - Documentation of core functions that cannot be accessed by persons with disabilities.

    - Documentation on how to configure and install the ICT Item to support accessibility.
    - Demonstration of the ICT Item's conformance to the applicable Section 508 Standards, (including the ability of the ICT Item to create electronic content – where applicable).

2. Before accepting ICT required under the contract, the government reserves the right to perform testing on required ICT items to validate the offeror's Section 508 conformance claims. If the government determines that Section 508 conformance claims provided by the offeror represent a higher level of conformance than what is actually provided to the agency, the government shall, at its option, require the offeror to remediate the item to align with the offeror's original Section 508 conformance claims prior to acceptance.

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.

Section 508 Requirements

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

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

Item that contains Information and Communications Technology (ICT): Enterprise Integration Services Modernization (EISM)

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

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

Applicable 508 requirements for electronic content features and components (including Internet and Intranet website): Does not apply

Applicable 508 requirements for software features and components (including Web, desktop, server, mobile client applications; Electronic content and software authoring tools and platforms; Software infrastructure): All WCAG Level AA Success Criteria, 502 Interoperability with Assistive Technology, 503 Application, 504 Authoring Tools

Applicable 508 requirements for hardware features and components (including Computers & laptops; Servers): All requirements apply

Applicable support services and documentation: All requirements apply

2. When providing and managing hosting services for ICT, the contractor shall ensure the hosting service does not reduce the item's original level of Section 508 conformance before providing the hosting service.
3. When providing installation, configuration or integration services for ICT, the contractor shall not reduce the original ICT item's level of Section 508 conformance prior to the services being performed.
4. When providing maintenance upgrades, substitutions, and replacements to ICT, the contractor shall not reduce the original ICT's level of Section 508 conformance prior to upgrade, substitution or replacement. The agency reserves the right to request an Accessibility Conformance Report (ACR) for proposed substitutions and replacements prior to acceptance. The ACR should be created using the on the Voluntary Product Accessibility Template Version 2.1 or later. The template can be located at https://www.itic.org/policy/accessibility/vpat
5. When developing or modifying ICT for the government, the contractor shall ensure the ICT fully conforms to the applicable Section 508 Standards. When modifying a commercially available or government-owned ICT, the contractor shall not reduce the original ICT Item's level of Section 508 conformance.
6. When developing or modifying web and software ICT, the contractor shall demonstrate Section 508 conformance by providing Section 508 test results based on the versions of the DHS Trusted Tester Methodology currently approved for use, as defined at https://www.dhs.gov/compliance-test-processes. The contractor shall use testers who are certified by DHS on how to use the DHS Trusted Tester Methodology (e.g "DHS Certified Trusted Testers") to conduct accessibility testing. Information on how testers can become certified is located at https://www.dhs.gov/publication/trusted-tester-resources.
7. When developing or modifying ICT that are delivered in an electronic Microsoft Office or Adobe PDF format, the contractor shall demonstrate conformance by providing Section 508 test results based on the Accessible Electronic Documents – Community of Practice (AED COP) Harmonized Testing Guidance at https://www.dhs.gov/compliance- test-processes.
8. Contractor personnel shall possess the knowledge, skills and abilities necessary to address the applicable revised Section 508 Standards for each ICT.
9. Exceptions for this work statement have been determined by DHS and only the exceptions described herein may be applied. Any request for additional exceptions shall be sent to the Contracting Officer and a determination will be made according to DHS Directive 139-05, Office of Accessible Systems and Technology, dated January 29, 2016 and DHS Instruction 139-05-001, Managing the Accessible Systems and Technology Program, dated January 11, 2017.
10. Where ICT conforming to one or more requirements in the Revised 508 Standards is not commercially available, the agency shall procure the ICT that best meets the Revised 508

Standards consistent with the agency's business needs, in accordance with 36 CFR E202.7. Any selection of a product or service that meets less accessibility standards due to a significant difficulty or expense shall only be permitted under an undue burden claim and requires authorization from the DHS Office of Accessible Systems and Technology (OAST) according to DHS Directive 139-05, Office of Accessible Systems and Technology, dated January 29, 2016 and DHS Instruction 139-05-001, Managing the Accessible Systems and Technology Program, dated January 11, 2017 and 36 CFR E202.6.

Staffing Mix