SOLICITATION/CONTRACT/ORDER FOR COMMERCIAL ITEMS

OFFEROR TO COMPLETE BLOCKS 12, 17, 23, 24, & 30

1. REQUISITION NUMBER	PAGE	OF
MULTIPLE	1	2

2. CONTRACT NO.	3. AWARD/ EFFECTIVE DATE	4. ORDER NUMBER	5. SOLICITATION NUMBER	6. SOLICITATION ISSUE DATE
GS00Q17GWD2017	27SEP19	70SBUR19F00000550		

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

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 US Citizenship & Immigration Svcs Office of Information Technology 111 Massachusetts Ave, NW Suite 5000 Washington DC 20529	HQOIT	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
REDHORSE CORPORATION 363 5TH AVENUE SUITE 201 SAN DIEGO CA 921016965 TELEPHONE NO.	808149004+0000		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: 808149004+0000 ---- This is a Directed Task Order under the GSA S(a) STARS II contract for USCIS Records and SYstems integrated through iNtelligent Connectors (R-SYNC) ---- PART I - SF-1449(this document) PART II - CLAUSES AND TERMS PART III - DOCUMENTS, EXHIBITS, OR ATTACHMENTS *(Use Reverse and/or Attach Additional Sheets as Necessary)*				

25. ACCOUNTING AND APPROPRIATION DATA	26. TOTAL AWARD AMOUNT (For Govt. Use Only)
See schedule	[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 1 COPIES TO ISSUING OFFICE. CONTRACTOR AGREES TO FURNISH AND DELIVER ALL ITEMS SET FORTH OR OTHERWISE IDENTIFIED ABOVE AND ON ANY ADDITIONAL SHEETS SUBJECT TO THE TERMS AND CONDITIONS SPECIFIED.

☐ 29. AWARD OF CONTRACT _____ 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
[redacted]	[redacted]

30b. NAME AND TITLE OF SIGNER (Type or print)	30c. DATE SIGNED	31b. NAME OF CONTRACTING OFFICER (Type or print)	31c. DATE SIGNED
[redacted]	9/26/2019	[redacted]	27SEP19

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
	AAP Number: N/A Accounting Info: CDOSTRG 001 EP 20-05-00-000 23-20-0600-00-00-00-00 GE-25-86-00 000000 Period of Performance: 09/30/2019 to 09/29/2020				
0001	DevSecOps Team 1 Firm-Fixed Price PSC: D308 Period of Performance: 09/30/2019 - 09/29/2020	12	MO	[redacted]	[redacted]
0002	DevSecOps Team 2 Firm-Fixed Price PSC: D308 Period of Performance: 09/30/2019 - 09/29/2020	12	MO	[redacted]	[redacted]
0003	DevSecOps Team 3 Firm-Fixed Price PSC: D308 Period of Performance: 09/30/2019 - 09/29/2020	12	MO	[redacted]	[redacted]
	The total amount of award: [redacted]. The obligation for this award is shown in box 26.				

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. MA LING ADDRESS OF AUTHORIZED GOVERNMENT REPRESENTATIVE	32f. TELEPHONE NUMBER OF AUTHORIZED GOVERNMENT REPRESENTATIVE 32g. E-MA L OF AUTHORIZED GOVERNMENT REPRESENTATIVE

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

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

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

PART II – CONTRACT CLAUSES AND TERMS

THIS ORDER WILL BE SUBJECT TO THE CONTRACTOR'S GSA STARS II IDIQ CONTRACT TERMS AND CONDITIONS

FAR 52.252-2 -- CLAUSES INCORPORATED BY REFERENCE (FEB 1998)

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

FAR Number	Title	Date
52.203-19	PROHIBITION ON REQUIRING CERTAIN INTERNAL CONFIDENTIALITY AGREEMENTS OR STATEMENTS	JAN 2017
52.204-18	COMMERCIAL AND GOVERNMENT ENTITY CODE MAINTENANCE	Jul 2016
52.204-19	INCORPORATION BY REFERENCE OF REPRESENTATIONS AND CERTIFICATIONS	Dec 2014
52.224-3	PRIVACY TRAINING	JAN 2017
52.227-14	RIGHTS IN DATA - GENERAL	MAY 2014
52.232-39	UNENFORCEABILITY OF UNAUTHORIZED OBLIGATIONS	JAN 2013
52.237-3	CONTINUITY OF SERVICES	JAN 1991

FAR incorporated in full text

52.204-25 Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment (AUG 2019)

(a) Definitions. As used in this clause--
Covered foreign country means The People's Republic of China.
Covered telecommunications equipment or services means--

(1) Telecommunications equipment produced by Huawei Technologies Company or ZTE Corporation (or any subsidiary or affiliate of such entities);
(2) For the purpose of public safety, security of Government facilities, physical security surveillance of critical infrastructure, and other national security purposes, video surveillance and telecommunications equipment produced by Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company (or any subsidiary or affiliate of such entities);
(3) Telecommunications or video surveillance services provided by such entities or using such equipment; or
(4) Telecommunications or video surveillance equipment or services produced or provided by an entity that the Secretary of Defense, in consultation with the Director of National Intelligence or the Director of the Federal Bureau of Investigation, reasonably believes to be an entity owned or controlled by, or otherwise connected to, the government of a covered foreign country.

Critical technology means--

(1) Defense articles or defense services included on the United States Munitions List set forth in the International Traffic in Arms Regulations under subchapter M of chapter I of title 22, Code of Federal Regulations;
(2) Items included on the Commerce Control List set forth in Supplement No. 1 to part 774 of the Export Administration Regulations under subchapter C of chapter VII of title 15, Code of Federal Regulations, and controlled--
    i. Pursuant to multilateral regimes, including for reasons relating to national security, chemical and biological weapons proliferation, nuclear nonproliferation, or missile technology; or
    ii. For reasons relating to regional stability or surreptitious listening;
(3) Specially designed and prepared nuclear equipment, parts and components, materials, software, and technology covered by part 810 of title 10, Code of Federal Regulations (relating to assistance to foreign atomic energy activities);
(4) Nuclear facilities, equipment, and material covered by part 110 of title 10, Code of Federal Regulations (relating to export and import of nuclear equipment and material);
(5) Select agents and toxins covered by part 331 of title 7, Code of Federal Regulations, part 121 of title 9 of such Code, or part 73 of title 42 of such Code; or
(6) Emerging and foundational technologies controlled pursuant to section 1758 of the Export Control Reform Act of 2018 (50 U.S.C. 4817). Substantial or essential component means any component necessary for the proper function or performance of a piece of equipment, system, or service.

(b) Prohibition. Section 889(a)(1)(A) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232) prohibits the head of an executive agency on or after August 13, 2019, from procuring or obtaining, or extending or renewing a contract to procure or obtain, any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system. The Contractor is prohibited from providing to the Government any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system, unless an exception at paragraph (c) of this clause applies or the covered telecommunication equipment or services are covered by a waiver described in Federal Acquisition Regulation 4.2104.

(c) Exceptions. This clause does not prohibit contractors from providing--
(1) A service that connects to the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements; or
(2) Telecommunications equipment that cannot route or redirect user data traffic or permit visibility into any user data or packets that such equipment transmits or otherwise handles.

(d) Reporting requirement.
(1) In the event the Contractor identifies covered telecommunications equipment or services used as a substantial or essential component of any system, or as critical technology as part of any system, during contract performance, or the Contractor is notified of such by a subcontractor at any tier or by any other source, the Contractor shall report the information in paragraph (d)(2) of this clause to the Contracting Officer, unless elsewhere in this contract are established procedures for reporting the information; in the case of the Department of Defense, the Contractor shall report to the website at https://dibnet.dod.mil. For indefinite delivery contracts, the Contractor shall report to the Contracting Officer for the indefinite delivery contract and the Contracting Officer(s) for any affected order or, in the case of the Department of Defense, identify both the indefinite delivery contract and any affected orders in the report provided at https://dibnet.dod.mil.

(2) The Contractor shall report the following information pursuant to paragraph (d)(1) of this clause:

i. Within one business day from the date of such identification or notification: The contract number; the order number(s), if applicable; supplier name; supplier unique entity identifier (if known); supplier Commercial and Government Entity (CAGE) code (if known); brand; model number (original equipment manufacturer number, manufacturer part number, or wholesaler number); item description; and any readily available information about mitigation actions undertaken or recommended.

ii. Within 10 business days of submitting the information in paragraph (d)(2)(i) of this clause: Any further available information about mitigation actions undertaken or recommended. In addition, the Contractor shall describe the efforts it undertook to prevent use or submission of covered telecommunications equipment or services, and any additional efforts that will be incorporated to prevent future use or submission of covered telecommunications equipment or services.

(e) Subcontracts. The Contractor shall insert the substance of this clause, including this paragraph (e), in all subcontracts and other contractual instruments, including subcontracts for the acquisition of commercial items.

(End of Clause)

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

The Government may require continued performance of any services within the limits and at the rates specified in the contract. These rates may be adjusted only as a result of revisions to prevailing labor rates provided by the Secretary of Labor. The option provision may be exercised more than once, but the total extension of performance hereunder shall not exceed **6** months. The Contracting Officer may exercise the option by written notice to the Contractor within **15** days.

(End of Clause)

52.219-14 Limitations on Subcontracting (DEVIATION 2019-01)

(a) This clause does not apply to the unrestricted portion of a partial set-aside.

(b) *Definition.* As used in this clause—

"Similarly situated entity" means a first-tier subcontractor, including an independent contractor, that has the same small business program status as that which qualified the prime contractor for the award, and that is considered small for the NAICS code the prime contractor assigned to the subcontract the subcontractor will perform. An example of a similarly situated entity is a first-tier subcontractor that is a HUBZone small business concern for a HUBZone set- aside or sole source award under the HUBZone Program.

(c) *Applicability.* This clause applies only to—

(1) Contracts that have been set aside or reserved any of the small business concerns identified in 19.000(a)(3);

(2) Part or parts of a multiple-award contract that have been set aside for any of the small business concerns identified in 19.000(a)(3);

(3) Contracts that have been awarded on a sole-source basis in accordance with subparts 19.8, 19.13, 19.14, and 19.15; and

(4) Orders set aside for any of the small business concerns identified in 19.000(a)(3) under multiple-award contracts as described in 8.405-5 and 16.505(b)(2)(i)(F).

(d) *Independent contractors.* An independent contractor shall be considered a subcontractor.

(e) *Agreement.* By submission of an offer and execution of a contract, the Offeror/Contractor agrees in performance of the contract in the case of a contract for—

(1) Services (except construction), it will not pay more than 50 percent of the amount paid by the Government for contract performance to subcontractors that are not similarly situated entities. Any work that

a similarly situated entity further subcontracts will count toward the 50 percent subcontract amount that cannot be exceeded;

(2) Supplies (other than procurement from a nonmanufacturer of such supplies), it will not pay more than 50 percent of the amount paid by the Government for contract performance, excluding the cost of materials, to subcontractors that are not similarly situated entities. Any work that a similarly situated entity further subcontracts will count toward the 50 percent subcontract amount that cannot be exceeded;

(3) General construction, it will not pay more than 85 percent of the amount paid by the Government for contract performance, excluding the cost of materials, to subcontractors that are not similarly situated entities. Any work that a similarly situated entity further subcontracts will count toward the 85 percent subcontract amount that cannot be exceeded; or

(4) Construction by special trade contractors, it will not pay more than 75 percent of the amount paid by the Government for contract performance, excluding the cost of materials, to subcontractors that are not similarly situated entities. Any work that a similarly situated entity further subcontracts will count toward the 75 percent subcontract amount that cannot be exceeded.

(f) A joint venture agrees that, in the performance of the contract, the applicable percentage specified in paragraph (e) of this clause will be performed by the aggregate of the joint venture participants.

(End of clause)

HSAR incorporated in full text

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

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 HS.

(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)

HSAR 3052.212-70 - Contract Terms and Conditions Applicable to DHS Acquisition of Commercial Items (Sep 2012)

The Contractor agrees to comply with any provision or clause that is incorporated herein by reference to implement agency policy applicable to acquisition of commercial items or components. The provision or clause in effect based on the applicable regulation cited on the date the solicitation is issued applies unless otherwise stated herein. The following provisions and clauses are incorporated by reference:

(a) Provisions.

HSAR Number	Title	Date
3052.209-72	ORGANIZATIONAL CONFLICTS OF INTEREST.	SEP 2012

(b) Clauses.

HSAR Number	Title	Date
3052.205-70	ADVERTISEMENTS, PUBLICIZING AWARDS, AND RELEASES	SEP 2012
3052.222-70	STRIKES OR PICKETING AFFECTING TIMELY COMPLETION OF THE CONTRACT WORK	DEC 2003
3052.222-71	STRIKES OR PICKETING AFFECTING ACCESS TO A DHS FACILITY	DEC 2003
3052.242-72	CONTRACTING OFFICER'S TECHNICAL REPRESENTATIVE.	DEC 2003

(End of Clause)

HSAR 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 (*In accordance with the requirements of the Statement of Objectives*):

Data Science and AI/ML Specialist
Full-Stack Engineers
Business Analyst

(End of clause)

HSAR Deviation 15-01 INFORMATION TECHNOLOGY SECURITY AND PRIVACY TRAINING (MAR 2015)

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

b) Security Training Requirements.

a. 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.

b. 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 Attachment 6 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 email notification shall state the required training has been completed for

all Contractor and subcontractor employees.

(End of Clause)

HSAR Deviation 15-01 SAFEGUARDING OF SENSITIVE INFORMATION (MAR 2015)

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

(b) Definitions. As used in this clause—

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

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

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

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

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

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

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

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

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

(1) Truncated SSN (such as last 4 digits)
(2) Date of birth (month, day, and year)
(3) Citizenship or immigration status
(4) Ethnic or religious affiliation
(5) Sexual orientation
(6) Criminal History
(7) Medical Information
(8) System authentication information such as mother's maiden name, account passwords or personal identification numbers (PIN) Other PII may be "sensitive" depending on its context, such as a list of employees and their performance ratings or an unlisted home address or phone number. In contrast, a business card or public telephone directory of agency employees contains PII but is not sensitive.

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

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

Security and Privacy Controls for Federal Information Systems and Organizations accessible at http://csrc.nist.gov/publications/PubsSPs.html

(11) NIST Special Publication 800-88 Guidelines for Media Sanitization accessible at http://csrc.nist.gov/publications/PubsSPs.html

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

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

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

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

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

(e) Authority to Operate. The Contractor shall not input, store, process, output, and/or transmit sensitive information within a Contractor IT system without an Authority to Operate (ATO) signed by the Headquarters or Component CIO, or designee, in consultation with the Headquarters or Component Privacy Officer. Unless otherwise specified in the ATO letter, the ATO is valid for three (3) years. The Contractor shall adhere to current Government policies, procedures, and guidance for the Security Authorization (SA) process as defined below.

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

i. Security Authorization Process Documentation. SA documentation shall be developed using the Government provided Requirements Traceability Matrix and Government security documentation templates. SA documentation consists of the following: Security Plan, Contingency Plan, Contingency Plan Test Results, Configuration Management Plan,

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

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

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

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

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)

Other Task Order Requirements

1. 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.

2. DHS/USCIS SECURITY REQUIREMENTS CLAUSE 5

This clause is hereby incorporated under Part 3.3 of this notice – DHS/USCIS SECURITY REQUIREMENTS CLAUSE 5.

3. 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 Security Clause 5 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). This NTP will not be granted until sufficient personnel have EOD'd and full performance is reasonably expected to occur based upon the mix of personnel available to perform.

f) If all personnel have not received a favorable EOD within **90** days after task order award (at no fault of the contractor), the government reserves the right to seek consideration in all aspects of the task order.

4. EXPECTATION OF CONTRACTOR PERSONNEL

The government expects competent, productive, qualified IT professionals to be assigned to this task order. 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.

5. INVOICING INSTRUCTIONS

The vendor must submit all invoices in accordance with FAR 52.212-4(g)

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

If a paper invoice is submitted, mail the invoice to:
USCIS Invoice Consolidation
PO Box 1000, Williston, VT 05495

6. POSTING OF CONTRACT (OR ORDER) IN FOIA READING ROOM

The Government intends to post the contract (or order) resulting from this solicitation to a public FOIA reading room. Within 30 days of award, the Contractor shall submit a redacted copy of the executed contract (or order) (including all attachments) suitable for public posting under the provisions of the Freedom of Information Act (FOIA). The Contractor shall submit the documents to the USCIS FOIA Office by email at foiaerr.nrc@uscis.dhs.govwith a courtesy copy to the contracting officer.

7. ENTERPRISE ARCHITECHTURE (EA) COMPLIANCE LANGUAGE

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

Specifically, the contractor shall comply with the following Homeland Security (HLS) EA requirements:

- All developed solutions and requirements shall be compliant with the HLS EA principles
- All IT hardware and software shall be compliant with the HLS EA Technical Reference Model (TRM) Standards and Products Profile ; all products are subject to DHS Enterprise Architectural approval. No products may be utilized in any production environment that is not included in the HLS EA 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.

8. GOVERNMENT FURNISHED PROPERTY (GFP) *(handled in accordance with FAR 52.245-1 of your STARS II IDIQ contract)*

Only GFP laptops, mobile phones for key personnel, and PIV Cards will be issued and used in performing work on this contract. No personal or company owned storage devices, (thumb drives, DVDs, or CDs) will be used with the GFP. Computing keyboards, mice, monitors, printers and other peripherals will not be issued by the government. A webinar account, such as AT&T Connect, will be provided to the contractor to facilitate virtual demos and other meetings with stakeholders at various physical locations. Mobile devices may be provided as identified by the COR or Government Program Manager. GFI, such as USCIS design standards, will be provided to the contractor following award.

Equipment / Government Property	Date / Event Indicate when the GFP will be furnished	Date / Event Indicate when the GFP will be returned	Unit	Serial Number(s)	Manufacture & Model Number
Laptop MAC and Windows based	After EOD	Upon Departure	EA	TBD	Standard USCIS approved manufacturer
PIV Card	After EOD	Upon Departure	EA	TBD	Standard USCIS approved manufacturer
Mobile Phone-if deemed necessary by the government	After EOD	Upon Departure	EA	TBD	Standard USCIS approved manufacturer

9. PLACE OF PERFORMANCE

Contractor personnel employed under this contract will primarily work from the contractor's facility(ies), but on as-needed basis will be required to report and work in-person to the U.S. National Capital Region.

PART III – DOCUMENTS, EXHIBITS, OR ATTACHMENTS

3.1 PERFORMANCE OF WORK STATEMENT

3.2 QUALITY ASSURANCE SURVEILLANCE PLAN

3.3 DHS/USCIS SECURITY REQUIREMENTS CLAUSE 5

3.1 PERFORMANCE OF WORK STATEMENT

Section 1 (S1) – OBJECTIVES, OVERVIEW, AND SCOPE

This is a nonpersonal services contract to provide agile software development services, including integration of machine learning approaches to enable adaptive/intelligent software, in support of the U.S. Security and Immigration Services (USCIS) initiative to advance services and technologies using artificial intelligence and machine learning for connecting records and systems. It will be executed via tight coupling of software development, security, and operations (DevSecOps) and data science to rapidly deliver a minimum viable product (MVP). USCIS shall not exercise any supervision or control Contractor personnel, who shall be accountable solely to The contractor via the Project Manager (PM), who in turn is responsible to the Government's Product Manager.

1.1. DESCRIPTION OF SERVICES/INTRODUCTION: The contractor will provide all personnel, equipment, supplies, facilities, transportation, tools, materials, supervision, and other items and nonpersonal services necessary. The contractor will perform software development via government-specified agile frameworks and DevSecOps as defined in this Performance Work Statement (PWS), except for those items specified as government-furnished property and services.

1.2. BACKGROUND: USCIS has been transforming its citizenship verification and immigrant processing culture from paper-based to digital. In addition, there has been a rapid pace of industry innovation using artificial intelligence and machine learning approaches fueled by the integration of constantly changing and newly developed cloud services. To bridge the gap between the wealth of experience that industry brings and our capacity to adopt emerging capabilities, there exists a need to leverage industry to build out modern services in support of Identity, Records, and National Security Delivery (IRNSD).

1.3. OBJECTIVES: The goal of IRNSD is to establish an integrated, experienced agile development/data science team to:

- Stage the legacy data platform, connectors, and models.
- Provide adaptive integrated data access layer.
- Provide business-focused and intelligent searching and analytics.
- Provide transparent and traceable data lineage with granular data security and controls.
- Integrate data governance into the automated-first continuous integration/continuous delivery (CI/CD) pipeline.
- Provide models and algorithms that consume snapshots and continuous flows of data to connect disparate systems.

To achieve these goals, The contractor will establish and execute new services within the currently approved USCIS architecture and tools. The contractor may propose new open source and/or commercially available tools or technologies, and USCIS Security standards & USCIS software licensing will vet and, if appropriate, acquire any proposed new tools.

1.4. SCOPE: The contractor will provide Agile Project Management, Design Thinking, User Interface/User Experience (UI/UX) Design and Testing, as well as Agile Software Development

and Data Science Services. The contractor will deliver an MVP as defined by the USCIS product manager, to include:

- System design documentation on a USCIS Internal Software Design Document wiki page, as well as scripts for manual testing when appropriate.
- Documentation and stories on the USCIS Confluence and JIRA sites.
- All code and scripting for the solution in the USCIS code repository, currently GitHub.

1.5. PERIOD OF PERFORMANCE: The period of performance for this contract encompasses a base period of 12 months.

Base period: 09/30/2019 – 09/29/2020

1.6. GENERAL INFORMATION

1.6.1. Quality Control: The contractor will maintain an effective quality control program to ensure services are performed in accordance with standards outlined in this document. The contractor will develop and implement procedures to identify, prevent, and ensure non-recurrence of defective services, and ensure our work complies with the requirements of the contract.

1.6.2. Quality Assurance: USCIS will evaluate the contractor's performance under this contract in accordance with the Quality Assurance Surveillance Plan (QASP), which shall be tailored to the Quality Control Plan (QCP). The QASP (see Part 7) plan is primarily focused on what the Government must do to ensure that the contractor has performed according to the performance standards. It defines how the performance standards will be applied, the frequency of surveillance, and the minimum acceptable defect rate(s).

1.6.3. Recognized Holidays:

New Year's Day	Labor Day
Martin Luther King Jr.'s Birthday	Columbus Day
President's Day	Veteran's Day
Memorial Day	Thanksgiving Day
Independence Day	Christmas Day

1.6.4. Hours of Operation: The contractor will provide support to this effort between the hours of 8:00AM and 4:30PM Monday through Friday except Federal holidays or when the Government facility is closed due to local or national emergencies, administrative closings, or similar

Government-directed facility closings. The contractor will maintain an adequate workforce for the uninterrupted performance of tasks defined within this PWS when the Government facility is not closed for the above reasons. The contractor will provide stability and continuity of the workforce.

1.6.5. Place of Performance: The work to be performed under this contract will be performed at the Contractor facility at 1777 N Kent Street, Suite 1200 Arlington VA 22209. The contractor and subcontractor personnel may work from remote work locations in the United States as coordinated through the Contracting Officer's Representative (COR).

1.6.6. Security Requirements:

1.6.6.1. Personnel Security. 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. This requirement includes U.S. Citizenship and successful completion of a Department of Homeland Security (DHS) background check.

1.6.6.2. Corporate Security Officer. The contractor will designate a Corporate Security Officer. The individual will interface with the USCIS Office of Security and Integrity through the Contracting Officer's Representative (COR) on all security matters, to include physical security, personnel security, and protection of all Government information and data accessed by the Contractor.

1.6.6.3. Inspection. The COR 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.

1.6.6.4. Physical Security. Contractor will be responsible for safeguarding government equipment, information, and property provided for contractor use. At the close of each work period, government equipment and materials will be secured within The contractor's access-controlled facilities.

1.6.6.5. Key Control. The contractor will establish and implement methods of making sure all keys/key cards issued to the Contractor by the Government are not lost or misplaced and are not used by unauthorized persons. In the event of loss, The contractor will document the incident and notify the government in accordance with USCIS security policy.

1.6.7. Post-Award Conference/Periodic Progress Meetings: The Contractor agrees to attend any post-award conference convened by the contracting activity or contract administration office in accordance with Federal Acquisition Regulation (FAR) Subpart 42.5. The contracting officer, COR, and other Government personnel, as appropriate, may meet periodically with the contractor to review the Contractor's performance. At these meetings, the contracting officer will apprise the Contractor of how the government views the Contractor's performance and the Contractor will apprise the Government of problems, if any, being experienced. Appropriate

action shall be taken to resolve outstanding issues. These meetings shall be at no additional cost to the government.

1.6.8. Contracting Officer's Representative: The contractor acknowledges that the COR will be identified by separate letter. The COR monitors all technical aspects of the contract and assists in contract administration. The COR is authorized to perform the following functions: assure that the Contractor performs the technical requirements of the contract; perform inspections necessary in connection with contract performance; maintain written and oral communication with the Contractor concerning technical aspects of the contract; issue written interpretations of technical requirements, including Government drawings, designs, specifications; monitor Contractor's performance and notify both the Contracting Officer and Contractor of any deficiencies; coordinate availability of government furnished property; and provide site entry of Contractor personnel. A letter of designation issued to the COR, a copy of which is sent to the Contractor, states the responsibilities and limitations of the COR, especially regarding changes in cost or price, estimates, or changes in delivery dates. The COR is not authorized to change any of the terms and conditions of the resulting order.

1.6.9. Key Personnel: The following positions are proposed as key personnel, as listed below:

1.6.9.1. Contract Manager. The contractor will designate a contract manager who shall be responsible for the performance of the work. The Project Manager shall act for the contractor when the manager is absent. The contract manager or alternate shall have full authority to act for the contractor on all contract matters relating to daily operation of this contract. The contract manager or alternate shall be available between 8:00 A.M. to 4:30 P.M. ET Monday through Friday except Federal holidays or when the government facility is closed for administrative reasons.

1.6.9.2. Data Science and Artificial Intelligence/Machine Learning (AI/ML) Specialist. The contractor will propose the Data Science and AI/ML Specialist position as key. Personnel filling this role shall possess:

- A minimum of five (5) years of experience in the information technology field focusing on AI/ML development projects, DevSecOps and technical architecture specifically.
- Strong architecture & design experience, including at least three (3) years of experience deploying production enterprise applications in AWS that use AI/ML.
- Expertise in large scale, high performance enterprise big data application deployment and solution architecture on complex heterogeneous environments in AWS.
- A bachelor's degree in Computer Science, Information Technology Management, or Engineering, or other comparable degree(s) or experience.

1.6.9.3. Full-Stack Engineer. The contractor will propose a Full-Stack Engineer position as key. Personnel filling this role shall possess:

- A minimum of five (5) years of experience in the information technology field focusing on AI/ML development projects using DevSecOps and AWS cloud environments.

- Strong full stack engineering, including at least three (3) years of experience deploying production enterprise applications in AWS that use AI/ML.
- At least three (3) years of specific software engineering related to front-end and back-end applications and or data services.
- Experience in large scale, high performance enterprise big data application deployment and solution architecture on complex heterogeneous environments in AWS.

1.6.9.4. Business Analyst. The contractor proposes the Business Analyst position as key. Personnel filling this role shall possess:

- A minimum of three (3) years of experience focusing on business architecture analysis and UI/UX design.
- Minimum experience of one (1) year in building business process models, writing acceptance criteria, and designing user interfaces for a production system.

1.6.11. Identification of Contractor Employees: All Contractor personnel attending meetings at Government site and working in other situations where their contractor status is not obvious to third parties will identify themselves as such to avoid creating an impression in the minds of members of the public that they are Government officials. Contractor personnel will also ensure that all documents or reports delivered are suitably marked as contractor products or that contractor participation is appropriately disclosed.

1.6.12. Phase In. To minimize a decrease in productivity and prevent negative impact on additional services, The contractor will nominate personnel for entry on duty (EOD) expediently during the phase-in period. 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). Contractor acknowledges the notice to proceed (NTP) will not be granted until sufficient personnel have entered on duty and full performance is reasonably expected to occur based upon the mix of personnel available to perform.

S2: DEFINITIONS & ACRONYMS

2. DEFINITIONS AND ACRONYMS:

2.1 DEFINITIONS:

2.1.1 CONTRACTOR. A supplier or vendor awarded a contract to provide specific supplies or service to the government. The term used in this contract refers to the prime.

2.1.2 CONTRACTING OFFICER. A person with authority to enter into, administer, and or terminate contracts, and make related determinations and findings on behalf of the government. Note: The only individual who can legally bind the government.

2.1.3 CONTRACTING OFFICER'S REPRESENTATIVE (COR). An employee of the U.S. Government appointed by the contracting officer to administer the contract. Such appointment

shall be in writing and shall state the scope of authority and limitations. This individual has authority to provide technical direction to the Contractor as long as that direction is within the scope of the contract, does not constitute a change, and has no funding implications. This individual does NOT have authority to change the terms and conditions of the contract.

2.1.4 DEFECTIVE SERVICE. A service output that does not meet the standard of performance associated with the Performance Work Statement.

2.1.5 DELIVERABLE. Anything that can be physically delivered; may include non-manufactured things such as meeting minutes or reports.

2.1.6 KEY PERSONNEL. Contractor personnel that are evaluated in a source selection process and that may be required to be used in the performance of a contract by the Key Personnel listed in the PWS. When key personnel are used as an evaluation factor in best value procurement, an offer can be rejected if it does not have a firm commitment from the persons that are listed in the proposal.

2.1.7 PHYSICAL SECURITY. Actions that prevent the loss or damage of Government property.

2.1.8 QUALITY ASSURANCE. The government procedures to verify that services being performed by the Contractor are performed according to acceptable standards.

2.1.9 QUALITY ASSURANCE SURVEILLANCE PLAN (QASP). An organized written document specifying the surveillance methodology to be used for surveillance of contractor performance.

2.1.10 QUALITY CONTROL. All necessary measures taken by the Contractor to assure that the quality of an end product or service shall meet contract requirements.

2.1.11 SUBCONTRACTOR. One that enters into a contract with a prime contractor. The Government does not have privity of contract with the subcontractor.

2.1.12 WORK DAY. The number of hours per day the Contractor provides services in accordance with the contract.

2.1.13 WORK WEEK. Monday through Friday, unless specified otherwise.

2.2 ACRONYMS:

AI/ML	Artificial Intelligence/Machine Learning
CMMI	Capability Maturity Model Integration
CAGE	Commercial and Government Entity
CI/CD	Continuous integration/continuous delivery
COR	Contracting Officer’s Representative

COTR	Contracting Officer's Technical Representative
CA	Corrective action
DHS	Department of Homeland Security
DQP	Director of Quality Programs
EIT	Electronic information & technology
EOD	Entry on duty
FAR	Federal Acquisition Regulation
GFI	Government-furnished information
IRNSD	Identity, Records, and National Security Delivery
ICT	Information communications technology
O&M	IT operations and maintenance
MVP	Minimum viable product
NTP	Notice to proceed
OAST	Office of Accessible Systems & Technology
OCI	Organizational Conflict of Interest
OEM	Original equipment manufacturer
PWS	Performance Work Statement
PIV	Personal identity verification
PO	Product Owner
PMP	Project Management Plan
PM	Project Manager
QASP	Quality Assurance Surveillance Plan
QCP	Quality Control Plan
QM	Quality Manager
DevSecOps	Software development, security, and operations
SME	Subject matter expert
UI/UX	User Interface/User Experience

S3: GOVERNMENT-FURNISHED PROPERTY, EQUIPMENT, AND SERVICES

3. GOVERNMENT-FURNISHED ITEMS AND SERVICES:

3.1 **Services**: USCIS will provide product management services including agile user stories and access to government systems, data, and experts to enable data understanding and subsequent performance of application development and data science work under this PWS.

3.2 **Facilities**: USCIS will provide facilities as needed for periodic meetings, collaboration, and demonstration.

3.3 **Utilities**: USCIS will provide access to and use of USCIS collaboration tools and repositories including Confluence, Jira, GitHub, and the USCIS internal Wiki.

3.4 **Equipment**: USCIS will provide laptops and mobile phones for key personnel, and personal identity verification (PIV) cards will be issued and used in performing work on this contract. No personal or company-owned storage devices (thumb drives, DVDs, or CDs) will be used with the government-furnished property. Computing keyboards, mice, monitors, printers, and other peripherals will not be issued by the government. A webinar account, such as AT&T Connect, will be provided to the Contractor to facilitate virtual demos and other meetings with stakeholders at various physical locations. Mobile devices may be provided as identified by the COR or Government Program Manager. Government-furnished information (GFI), such as USCIS design standards, will be provided to the Contractor following award.

3.5 **Materials**: USCIS will provide GFI to include copies of reference architectures and standards, database schemas, sample data, training data, and existing system technical specification. When appropriate, consistent with the Objectives statement in this PWS, Contractor may recommend new open-source and commercial tools or software to USCIS, who may elect to provide those as Government-Furnished Equipment/GFI.

S4: CONTRACTOR-FURNISHED ITEMS AND SERVICES

4. CONTRACTOR-FURNISHED ITEMS AND RESPONSIBILITIES:

4.1 **General**: Contractor shall furnish all supplies, equipment, facilities, and services required to perform work under this contract that are not listed under Part 3 of this PWS.

4.2 **Facility**: Contractor will provide its facility and maintain adequate facility security to ensure compliance with USCIS physical and personnel security requirements.

4.3 **Materials**: Contractor will provide all consumable materials such as pens, paper, markers, notepads, post-it notes, and other materials required in the performance of this effort.

4.4 **Equipment**: Contractor shall provide computing keyboards, mice, monitors, printers and other peripherals, and network connectivity.

4.5 **Training**: Contractor shall provide all training for personnel to include USCIS-mandated security training.

S5: SPECIFIC ROLES AND TASKS

5. SPECIFIC ROLES AND TASKS:

5.1 Basic Services. USCIS will provide product management and Contractor will provide an integrated DevSecOps team to deliver the MVP. As part of this team, Contractor will provide project management, business analysis, design thinking, UI/UX design, data science, and software development services via Agile methods. Contractor will deliver an MVP as defined by the USCIS Product Owner, including:

- System design documentation on a USCIS Internal Software Design Document wiki page, as well as scripts for manual testing when appropriate.
- Documentation and stories on the USCIS Confluence and JIRA sites.
- All code and scripting for the solution in the USCIS code repository, currently GitHub.

5.2 Roles and Tasks

5.2.1 Product Owner. A USCIS Product Owner will specify high-level requirements to this and other Contractor agile work teams. USCIS Product Owner will coordinate USCIS subject matter expert (SME) interaction with the Contractor team to define user stories and establish acceptance criteria. The acceptance criteria will specify expected functionality for a user story and any non-functional requirements to be met in the development of the story. The USCIS Product Owner, supported by USCIS SMEs and Business Analysts, will determine whether acceptance criteria have been satisfied.

5.2.2 DevSecOps Team

5.2.2.1 Project Manager (key). The Project Manager is the interface between the USCIS Product Owner and the DevSecOps team. The Project Manager will gather information from all stakeholders and integrate that information into a project plan, log production estimates, analyze historical performance and analyze programmers on their estimating accuracy, log task assignments, sustain a high rate of progress/production, remove impediments to work, and build and maintain the team culture.

5.2.2.2 Technical Lead (key). In addition to serving as a developer, the Technical Lead will resolve disagreements about technical architecture and ensure the technical architecture is consistent with USCIS/DHS guidelines and is maintained during development; ensure adherence to best practices, management processes, and other technical constraints; coordinate the day-to-day software development and data science work, and mentor other technical staff.

5.2.2.3 Developer. The Developer will analyze requirements, estimate production time, design solutions, code solutions, test solutions, and document work.

5.2.2.4 UX Designer. The UX Designer will understand the product owner's vision for the product, understand the business processes and user needs that the product supports, propose a

technical feasible UX design (both functional and visual), test the UX design with users in user research/feedback session, and incorporate user feedback into revised UX design.

5.2.2.5 Data Analyst. Research, analyze, and synthesize information about data sources; advise the developers and data scientists on business uses and value of the data, relationships between data sources, potential sources of data inaccuracy; advise developers and data scientists about data access and use policy and procedures.

5.2.2.6 Data Scientist and AI/ML Specialist (key). The Data Scientist and AI/ML Specialist leads data-science and machine-learning efforts, oversees exploratory data analysis of sample data sets, advises the technical lead on the incorporation of machine learning-developed inferencing models and workflows (e.g. dynamic retraining) into the application, mentors and guides the work of the data scientists, and consults with the UX designer and the technical lead on the incorporation of user-originated training data/metadata to support future machine learning projects.

5.2.2.7 Data Scientist. The Data Scientist is responsible for discovering insights from large amounts of structured and unstructured data; conducting data exploration, data cleaning, extract, translate and load activities, data enrichment, and aggregation; applying advanced statistical techniques to develop deep understanding and new insights from data; identifying, testing, evaluating and refining machine-learning techniques, documenting results, and developing alternate approaches.

5.2.2.8 Cloud Solution Architect. The Cloud Solution Architect advises the Technical Lead on cloud solutions architecture and cloud native services, especially related to scalability, application performance, and security.

5.2.2.9 Security Engineer. The Security Engineer participates in all phases of development as needed to identify, diagnose, and mitigate security risks as early and effectively as possible.

S6: ATTACHMENT/TECHNICAL EXHIBIT LISTING

6. ATTACHMENT/TECHNICAL EXHIBIT LIST:

6.1. Deliverables Schedule

6.2. Acceptance Criteria

TECHNICAL EXHIBIT 1

DELIVERABLES SCHEDULE

Deliverable	Frequency	# of Copies	Medium/Format	Submit To
Assessment of current data flows and connectors; gap identification	Within 30 days after notice to proceed (NTP)	One	MS Word via USCIS Internal Software Design Document wiki page	COR
Integrated end-to-end methodology and project roadmap	Within 30 days after NTP; updated as needed	One	MS Visio via USCIS Internal Software Design Document wiki page	COR
Data Architecture	Within 60 days after NTP; updated as needed	One	MS Visio via USCIS Internal Software Design Document wiki page	COR
Tickets and user stories	As completed	One each	USCIS internal Jira and Confluence page	COR
Application / environment source code	As completed	One each	USCIS code repository, currently GitHub	COR
Build scripts	As completed	One each	USCIS code repository, currently GitHub	COR
Machine learning workflow documentation	As completed	One each	Notebook format as appropriate via USCIS Internal Software Design Document wiki page	COR
Machine learning models	As completed	One each	USCIS code repository, currently GitHub	COR
Machine learning training data sets	As completed	One each	Storage infrastructure as designated by USCIS	COR

TECHNICAL EXHIBIT 2

ACCEPTANCE CRITERIA

Acceptance of software deliverables is defined as follows:

- Deliverable passes all new automated and manual acceptance tests that were defined before the most recent development iteration.
- Deliverable passes all prior automated and manual acceptance tests, verifying that no regression has occurred.
- Deliverable conforms to the "definition of done" that was defined before the iteration.

USCIS Product Owner (PO) will have a period of one week within an iteration ("Evaluation Period") after increments of a deliverable have been provided to verify that the Deliverable or part thereof is not deficient per acceptance criteria. The PO should notify Contractor prior to the expiration of the relevant Evaluation Period if the Deliverable or part thereof is deficient in any material respect (a "Nonconformity" pursuant to the definition of done or acceptance criteria agreed upon by the parties). The Contractor will correct such Nonconformity as soon as reasonably practical but no longer than the length of one iteration whereupon. The Government will receive an additional iteration period ("Verification Period") commencing upon its receipt of the corrected Deliverables or part thereof to verify that the specific Nonconformity has been corrected. The Contractor will also deliver the release test plan which is a step-by-step walkthrough of the functionality in the release and allows the user community to make notes and comments regarding how that functionality can be improved and made more useable or defect-free. The Contractor shall work to correct all errors and increase usability. Comments that are delivered within an agreed-upon number of days of the release walkthrough shall be included in the subsequent deliverable/release.

3.2 QUALITY ASSURANCE SURVEILLANCE PLAN (QASP)

1.1 INTRODUCTION

USCIS seeks *records and systems integrated through intelligent connectors* (R-SYNC) to enable digital service techniques that identify and solve core USCIS needs. R-SYNC will manage and integrate activities to successfully develop, monitor, maintain, and manage Agile teams through a complete DevSecOps lifecycle. The contractor's program management approach, founded on quality principles, is defined and maintained in its corporate quality management policy documents and tailored to best suit each contractor program, project, and task order.

1.2 DOCUMENT OVERVIEW AND PURPOSE

This QASP is considered a living document that will be referenced and updated consistently throughout the project to monitor and control the quality of project activity, directives, deliverables, and processes.

1.3 QUALITY ASSURANCE AND SURVEILLANCE PLAN IMPLEMENTATION

The R-SYNC QASP is initiated at the end of the transition period. During the transition period, the contractor will assume responsibility for quality assurance activities, establish project quality procedures and monitoring practices, inspect and tailor quality control measures, and ensure seamless transition of management and control practices.

This QASP is subject to ongoing updates and alignment based on task requirements and directives as determined by IRNSD.

All changes to this QASP shall be agreed to by the contractor's R-SYNC Project Manager for review and approval and to the Contracting Officer (CO) for approval and acceptance.

1.4 STAKEHOLDER ROLES AND RESPONSIBILITES

Table 2: Roles and Responsibilities

NAME	RESPONSIBILITY
Contractor Program Manager	Overseeing and tracking services in accordance with the performance standards of the Contract. Overseeing contractual internal quality management and quality assurance activities outlined in the Contractor R-SYNC QASP.
Contractor Task Manager(s)	Delivering services in accordance with the performance standards of the Contract. Conducting the internal quality management and quality assurance activities outlined in the Contractor R-SYNC QASP at the Task Order level.
Contractor Quality Assurance Manager	Responsible for overall quality management, oversight of quality initiatives, quality assurance practices, maintenance and inspection/auditing, and performance monitoring and reporting.

USCIS COTR	Assessing and reviewing contractor's performance under the Contract in relation to the performance standards detailed in the Contractor QASP.

1.5 COMMUNICATION PROCEDURES

Problems will be reported immediately to the Government, using the communications methods agreed between the designated points of contact as established, unless other criteria are determined by the COTR.

All contractor R-SYNC QASP activity and reporting requirements are delivered to the contractor PM monthly or at a frequency specified in the contract. Upon award of the contract and finalization of its requirements, this section of the QASP will be updated with reporting and communication schedules.

The contractor R-SYNC PM and Quality Manager (QM) shall meet monthly with contractor's corporate Director of Quality Programs (DQP) and the PMO to review quality activity.

1.6 CHANGE CONTROL PROCEDURES

This QASP is subject to revision, as necessary, throughout the life of the project. When changes are needed, Contractor R-SYNC QM reviews and revises the QASP before sending to the Contractor R-SYNC PM for approval. The previous version of the QASP will be archived, noting changes made, and the updated QASP will receive signatory approval from the QM.

Changes to this QASP must be reviewed and approved by the USCIS COTR.

All documentation associated with this QASP is subject to the procedural requirements defined within Contractor's internal *Document and Records Management System Procedure* manual.

2.0 QUALITY MANAGEMENT AND ASSURANCE

2.1 CONTRACTOR PROJECT QUALITY MANAGEMENT AND CONTROL OVERVIEW AND APPROACH

Contractor Corporation maintains a corporate ISO 9001:2015 certification for which all quality management and assurance practices are issued for Contractor projects. In addition, Contractor maintains a Capability Maturity Model Integration (CMMI) for Services Level 3 Rating for implementation of service, which applies defined and approved processes for project management, monitoring and control, and process improvement.

Contractor's DQP and Process & Program Manager provide oversight and input to the Contractor R-SYNC Quality Manager in relation to defined and approved Contractor quality processes and practice, as referenced under *Standards and Process Definitions* below. The Contractor R-SYNC QM manages and implements these quality processes and procedures at the project and task level, including monitoring quality initiatives and objectives related to project strategy and tasks.

Standards and Process Definitions: Application of quality process and procedure on the R-SYNC project is managed under defined Contractor quality procedures, which are ISO 9001:2015 compliant and certified. The following Contractor processes and/or procedural

documentation, at a minimum, are applied in their entirety, and tailored to specific Contractor R-SYNC project and task requirements:

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

Additional Contractor processes and procedures will be applied by the Contractor R-SYNC Team and the DQP as needed.

Management Review and Reporting: The Contractor R-SYNC PM and corporate DQP will meet on a quarterly basis to maintain a complete and continuous review of required quality assurance, monitoring, and control requirements. Based upon COTR and contract requirements, the quality program will report, at a minimum, the following data points on a monthly basis:

- Performance and conformity results for work product and services, based upon PWS objectives and contractual control requirements
- Technology reviews
- Change controls
- Testing activity and reporting
- Nonconformities and corrective action reporting and monitoring status
- Defined monitoring results
- Audit and inspection results
- Risk assessment and mitigation status

3.0 QUALITY ASSURANCE AND CONTROL MANAGEMENT

Upon startup of the Contractor R-SYNC Project Team, the quality program will assume responsibility for all quality assurance and control activity, as defined by contractual requirements and Contractor R-SYNC PM directive. Outlined below are initial control definitions, as per standard DevOps practices, within an Agile development environment.

Upon contract award, assignment of metrics and reporting parameters will be established once the final PWS has been approved. Assurance and performance measures will be assigned to PWS requirements, with updates to Section 3.1 below.

3.1 GOVERNMENT QUALITY ASSURANCE AND CONTROL SURVEILLANCE

Current planning for implementation and management of quality control practices are assigned under the following defined statement of work directives and objectives. The Contractor R-SYNC QM plans to support the following deliverable activities.

3.2 ASSESSMENT OF CURRENT DATE FLOWS AND CONNECTORS

Support gap assessment activity. This includes, but is not limited to:

- Conducting inspections – technical controls, legacy data platform evaluation.
- Audit against environment, operational, and regulatory compliance.
- Audit against stakeholder compliance.
- Data and records management.

3.3 DEVELOPMENT

Maintain quality oversight and assurance to ensure the following:

- Verification of integration within DevSecOps – centralized collaboration, data architecture and implementation.
- Efficiency of practice within agile environment.
- Code review and testing – defect management.
- Overall quality assurance through continuous integration and Sprints.

3.3.1 CHANGE CONTROL

Maintain quality oversight and compliance to ensure the following:

- Maintenance and change management practices for source code and build scripts, project documentation.
- Inspection/audit against procedural standards.
- Monitor collection of data measuring progress toward program goals.
- Verify and validate project activity.
- Support communication with defined stakeholders.

3.3.2 QUALITY ASSURANCE VERIFICATION VALIDATION ACTIVITY

Schedule and conduct continuous assurance checks:

- Sprints.
- Document reviews.
- Technology reviews, code reviews, etc.

3.3.3 ASSET MANAGEMENT

Provide asset management support, and records and information management support:

- Assist management of assets.
- Demonstrate continuous improvement.
- Comply with legal and regulatory requirements, including USCIS guidance.

3.3.4 INFORMATION AND TECHNOLOGY MANAGEMENT

Provide assistance for IT, record and information management, and information security support:

- Record and information management through all record lifecycles.
- Environmental and infrastructure data management: monitor and audit process and procedure.
- Information Technology Support: ensure governance, cyber security, IT operations and maintenance (O&M), and end user support practice and procedure is maintained and

compliant.

3.3.5 MISCELLANEOUS SUPPORT

Provide quality control and assurance support to the following areas:

- Program-wide support: Quality assurance on execution of tasks, document and records management.
- Information technology support: Information security management and NIST 800-171 compliance.
- Business support: Monitor effectiveness of process and procedure.
- Risk management and mitigation: Support process and practice, including performance of risk assessment, monitoring, and mitigation.

CONTROL #	PERFORMANCE ACTIVITY	TASK ASSIGNMENT
1	Inspect/Audit – Procedure, Work Products (QA), contract requirements: root cause analysis, mitigation and corrective action. • Report and manage corrective action • Verification/validation reporting • Baseline reporting • Compliance auditing and reporting	3.1.1, 3.1.2, 3.1.3, 3.1.4, 3.1.5, 3.1.6, 3.1.7
2	Risk assessment and prioritization: perform, mitigate, monitor, and report.	3.1.7
3	Establishment of Identification and Prevention Program: control of nonconforming product and defects.	3.1.1, 3.1.2

4.0 QASP PERFORMANCE REQUIREMENTS

4.1 QUALITY MANAGEMENT AND CONTROL ACTIVITIES

Quality management activity will focus on monitoring performance to ensure contract requirements are met and that problems with process management and defect prevention are identified and corrected if they hinder project objectives. This surveillance practice will be scheduled against the Contractor Project Management Plan (PMP), and any additional integrated management practices that require control and assurance practice.

In addition, the Contractor R-SYNC project will employ contract performance measures, which will be effectively measured, tracked, analyzed, and reported. The initial seven (7) quality controls identified within this plan will support overall quality assurance monitoring and evaluation of performance (surveillance). Additional requirements and/or adjustments to defined controls within this plan will be updated through the change management practices established on the project and highlighted in Section 1.7 above.

At a minimum the following activities will be managed by the Contractor R-SYNC QM.

4.1.1 SELF-INSPECTION – AUDIT PLAN

The Contractor R-SYNC Quality Manager will establish a master inspection/audit schedule that will be published and available to all Contractor R-SYNC project stakeholders. At a minimum,

the overall schedule will establish an annual plan for the following activities:

All Control activities defined in Section 3, including:

AUDIT/INSPECTION TYPE	REPORT	FREQUENCY
Internal process and procedural audits	• Audit Report • Corrective Action Report	• Annual
Work product – quality assurance reviews	• QA Report	• Upon completion, prior to delivery
Baseline Configuration audits	• Baseline Report	• Per release
Risk Assessments	• Risk Assessment and Treatment Plan	• Semi-annual
Corporate DQP Audit & Management Reviews	• Audit Report • Corrective Action Report • Management Reviews	• Audit – Annually • Corrective Action – Quarterly • Management Reviews – Semi-annual

This schedule and plan will be synchronized with the Contractor R-SYNC PMP, with frequency and specific date assignments post contract award, and validated against Customer requirements, logistics, and approval.

4.2 CORRECTIVE ACTION

The Contractor R-SYNC QASP implements a fully functional and certified corrective action process. Provided here-in is a summary of procedural practice from Contractor's *Corrective and Preventive Actions Procedure*.

4.3 IDENTIFICATION OF CORRECTIVE AND PREVENTIVE ACTIONS

Project and contract staff, while carrying out their assigned responsibilities, are likely to identify most problems or nonconformities via peer reviews, assessments, inspections, and audits. When Contractor R-SYNC project staff identify a problem or nonconformity, the team works with the Quality Manager to enter it in the corrective action (CA) log or submit a record of analysis.

4.4 SOURCES OF INFORMATION FOR CORRECTIVE AND PREVENTIVE ACTION ACTIVITIES

For existing nonconformities and for analyses that may identify preventive actions, the primary sources of information are:

- Inspection, assessment, audit
- Customer complaints, customer feedback
- Findings categorized as "observations" by 3rd party regulators
- Management review meeting reports
- Testing – defect

- Continual improvement process
- Suggestions from Contractor project team and/or the Customer
- Nonconforming services – disposition including customer acceptance with or without correction or amendment of requirements

4.5 CORRECTIVE ACTIONS

CAs are documented in a CA log and monitored by the Contractor R-SYNC QM, who assigns an owner and a response due date. The person assigned determines the root cause and the action necessary to resolve the problem. The following data is to be included on the CA log:

- ***ID #*** – unique identifying number
- ***Date*** – date action opened
- ***Source*** – to include inspection, audit, etc.
- ***Type of Action*** – to include corrective action, opportunity for improvement, etc.
- ***Auditor/Originator*** – name of individual identifying the issue
- ***Description*** – detailed information about the issue
- ***Responsible Person*** – individual responsible for managing and closing out the issue
- ***Due Date/Closed Date*** – planned and actual dates for closing out the issue
- ***Review Date (Planned/Actual)*** – planned and actual dates for verifying the effectiveness of the planned action
- ***Analysis/Root Cause*** – detailed information about the cause
- ***Planned Action*** – document the formal correction to the non-conformance to prevent recurrence
- ***Effectiveness of Action*** – review of action taken to verify that the corrective action is giving the expected result to preclude recurrence

4.6 ESCALATION PROCESS

The Contractor R-SYNC QM reviews open CAs on a monthly basis with the Contractor PM to identify delinquent reports. When timely and/or effective corrective actions are not achieved, and an extension has not been requested by the responsible party, the Contractor R-SYNC QM will formally escalate to the PM for additional resource and management oversight.

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

SECURITY REQUIREMENTS

GENERAL

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

FITNESS 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 Fitness authorization will follow as a result thereof. The granting of a favorable EOD decision or a full employment Fitness 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 Fitness 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. Additional Questions for Public Trust Positions – Branching
2. DHS Form 11000-6, Conditional Access to Sensitive But Unclassified Information Non-Disclosure Agreement
3. FD Form 258, Fingerprint Card **(2 cards)**
4. Form DHS 11000-9, Disclosure and Authorization Pertaining to Consumer Reports Pursuant to the Fair Credit Reporting Act
5. DHS Form 11000-25 Contractor Fitness/Security Screening Request Form
6. USCIS Continuation Page to DHS Form 11000-25
7. OF 306, Declaration for Federal Employment (approved use for Federal Contract Employment)
8. 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.

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 or on any security form listed above.

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.