ORDER FOR SUPPLIES OR SERVICES

PAGE OF PAGES: 1 of 11

IMPORTANT: Mark all packages and papers with contract and/or order numbers.

1. DATE OF ORDER: 09/25/2017	2. CONTRACT NO. (If any): HSHQDC-13-D-E2075
3. ORDER NO.: HSSCCG-17-J-00112	4. REQUISITION/REFERENCE NO.:

5. ISSUING OFFICE (Address correspondence to):
Department of Homeland Security
US Citizenship & Immigration Svcs
Office of Information Technology
111 Massachusetts Ave, NW
Suite 5000
Washington DC 20529

6. SHIP TO:
a. NAME OF CONSIGNEE: Department of Homeland Security
b. STREET ADDRESS: US Citizenship & Immigration Svcs
Office of Information Technology
111 Massachusetts Ave, NW
Suite 5000
c. CITY: Washington | d. STATE: DC | e. ZIP CODE: 20529

7. TO:
a. NAME OF CONTRACTOR: SEVATEC INC
b. COMPANY NAME:
c. STREET ADDRESS: 3112 FAIRVIEW PARK DRIVE
d. CITY: FALLS CHURCH | e. STATE: VA | f. ZIP CODE: 220424504

f. SHIP VIA:

8. TYPE OF ORDER
☐ a. PURCHASE — REFERENCE YOUR: Please furnish the following on the terms and conditions specified on both sides of this order and on the attached sheet, if any, including delivery as indicated.
☒ b. DELIVERY — Except for billing instructions on the reverse, this delivery order is subject to instructions contained on this side only of this form and is issued subject to the terms and conditions of the above-numbered contract.

9. ACCOUNTING AND APPROPRIATION DATA: See Schedule	10. REQUISITIONING OFFICE: HQCIS

11. BUSINESS CLASSIFICATION (Check appropriate box(es))
☒ a. SMALL ☐ b. OTHER THAN SMALL ☐ c. DISADVANTAGED ☐ d. WOMEN-OWNED ☐ e. HUBZone
☐ f. SERVICE-DISABLED VETERAN-OWNED ☐ g. WOMEN-OWNED SMALL BUSINESS (WOSB) ELIGIBLE UNDER THE WOSB PROGRAM ☐ h. EDWOSB

12. F.O.B. POINT:

13. PLACE OF		14. GOVERNMENT B/L NO.	15. DELIVER TO F.O.B. POINT ON OR BEFORE (Date)	16. DISCOUNT TERMS
a. INSPECTION: Destination	b. ACCEPTANCE: Destination		10/16/2017	Net 30

17. SCHEDULE (See reverse for Rejections)

ITEM NO. (a)	SUPPLIES OR SERVICES (b)	QUANTITY ORDERED (c)	UNIT (d)	UNIT PRICE (e)	AMOUNT (f)	QUANTITY ACCEPTED (g)
	DUNS Number: 132599668+0000 This is a Firm Fixed Price Task order for Identity, Credential and Access Management Unified-Services (ICAM-US) for the USCIS Office of Information Technology. The Period of Performance (PoP) consist of a Continued ...					

18. SHIPPING POINT	19. GROSS SHIPPING WEIGHT	20. INVOICE NO.	17(h) TOTAL (Cont. pages)
21. MAIL INVOICE TO: a. NAME: See Invoicing Instructions			[redacted]
SEE BILLING INSTRUCTIONS ON REVERSE — b. STREET ADDRESS (or P.O. Box)			17(i) GRAND TOTAL [redacted]
c. CITY	d. STATE	e. ZIP CODE	

22. UNITED STATES OF AMERICA BY (Signature): Charles E. Julian 9-25-17
23. NAME (Typed): CHARLES E. JULIAN
TITLE: CONTRACTING/ORDERING OFFICER

AUTHORIZED FOR LOCAL REPRODUCTION
PREVIOUS EDITION NOT USABLE

OPTIONAL FORM 347 (Rev. 2/2012)
Prescribed by GSA/FAR 48 CFR 53.213(f)

IMPORTANT: Mark all packages and papers with contract and/or order numbers.

DATE OF ORDER	CONTRACT NO.	ORDER NO.
09/25/2017	HSHQDC-13-D-E2075	HSSCCG-17-J-00112

ITEM NO. (a)	SUPPLIES/SERVICES (b)	QUANTITY ORDERED (c)	UNIT (d)	UNIT PRICE (e)	AMOUNT (f)	QUANTITY ACCEPTED (g)
	two month transition in period, a 10-month base period and three 12-month option periods for a total not to exceed 48 months. AAP Number: None DO/DPAS Rating: NONE Period of Performance: 09/26/2017 to 09/25/2021					
0001	Phase-In, section 6.5 of the PWS (FFP) Accounting Info: ITICISD 000 EX 200100000 2320030000000000GE253700 000000 Funded: [redacted]				[redacted]	
0002	Administrative Task Area, section 6.1 of the PWS (FFP) Accounting Info: ITICISD 000 EX 200100000 2320030000000000GE253700 000000 Funded: [redacted]				[redacted]	
0003	ICAM Enterprise Task Area, section 6.2 of the PWS (FFP) Accounting Info: ITICISD 000 EX 200100000 2320030000000000GE253700 000000 Funded: [redacted] Accounting Info: ITICAM0 000 EP 200500000 2320050000000000 GE258000 000000 Funded: [redacted]				[redacted]	
0004	ICAM Public Task Area, section 6.3 of the PWS (FFP) Accounting Info: ITICAM0 000 EP 200500000 2320050000000000 GE258000 000000 Funded: [redacted]				[redacted]	
0005	ICAM Legacy Integration Task Area, section 6.4 of the PWS (FFP) Accounting Info: Continued ...				[redacted]	

TOTAL CARRIED FORWARD TO 1ST PAGE (ITEM 17(H)) $7,251,756.80

IMPORTANT: Mark all packages and papers with contract and/or order numbers.

DATE OF ORDER	CONTRACT NO.	ORDER NO.
09/25/2017	HSHQDC-13-D-E2075	HSSCCG-17-J-00112

ITEM NO. (a)	SUPPLIES/SERVICES (b)	QUANTITY ORDERED (c)	UNIT (d)	UNIT PRICE (e)	AMOUNT (f)	QUANTITY ACCEPTED (g)
	ITICAM0 DPS EX 200100000 2320060000000000 GE258600 000000 Funded: [redacted]					
1002	Administrative Task Area, section 6.1 of the PWS (FFP) Amount: [redacted] Anticipated Exercise Date:08/01/2018				[redacted]	
1003	ICAM Enterprise Task Area, section 6.2 of the PWS (FFP) Amount: [redacted] Anticipated Exercise Date:08/01/2018				[redacted]	
1004	ICAM Public Task Area, section 6.3 of the PWS (FFP) Amount: [redacted] Anticipated Exercise Date:08/01/2018				[redacted]	
1005	ICAM Legacy Integration Task Area, section 6.4 of the PWS (FFP) Amount: [redacted] Anticipated Exercise Date:08/01/2018				[redacted]	
2002	Administrative Task Area, section 6.1 of the PWS (FFP) Amount: [redacted] Anticipated Exercise Date:08/01/2019				[redacted]	
2003	ICAM Enterprise Task Area, section 6.2 of the PWS (FFP) Amount: [redacted] Anticipated Exercise Date:08/01/2019				[redacted]	
2004	ICAM Public Task Area, section 6.3 of the PWS (FFP) Continued ...				[redacted]	

TOTAL CARRIED FORWARD TO 1ST PAGE (ITEM 17(H)) $0.00

IMPORTANT: Mark all packages and papers with contract and/or order numbers.

DATE OF ORDER	CONTRACT NO.	ORDER NO.
09/25/2017	HSHQDC-13-D-E2075	HSSCCG-17-J-00112

ITEM NO. (a)	SUPPLIES/SERVICES (b)	QUANTITY ORDERED (c)	UNIT (d)	UNIT PRICE (e)	AMOUNT (f)	QUANTITY ACCEPTED (g)
	Amount: [redacted] [redacted] Anticipated Exercise Date:08/01/2019					
2005	ICAM Legacy Integration Task Area, section 6.4 of the PWS (FFP) Amount: [redacted] [redacted] Anticipated Exercise Date:08/01/2019				[redacted]	
3002	Administrative Task Area, section 6.1 of the PWS (FFP) Amount: [redacted] Anticipated Exercise Date:08/01/2020				[redacted]	
3003	ICAM Enterprise Task Area, section 6.2 of the PWS (FFP) Amount: [redacted] [redacted] Anticipated Exercise Date:08/01/2020				[redacted]	
3004	ICAM Public Task Area, section 6.3 of the PWS (FFP) Amount: [redacted] [redacted] Anticipated Exercise Date:08/01/2020				[redacted]	
3005	ICAM Legacy Integration Task Area, section 6.4 of the PWS (FFP) Amount: [redacted] [redacted] Anticipated Exercise Date:08/01/2020 COR:Josette Hodges josette.y.hodges@uscis.dhs.gov CS:Christopher Hatin christopher.c.hatin@uscis.dhs.gov CO:Charles Julian charles.e.julian@uscis.dhs.gov				[redacted]	
	TOTAL CARRIED FORWARD TO 1ST PAGE (ITEM 17(H))				$0.00	

All applicable terms, conditions and clauses contained in the referenced DHS Eagle II IDIQ HSHQDC-13-D-E2075 contract apply to this order.

Section C – Task Order Clauses

Federal Acquisition Regulation (FAR) clauses incorporated by reference

52.209-10 **Prohibition on Contracting with Inverted Domestics Corporation** (Nov 2015)

52.232-39 **Unenforceability of Unauthorized Obligations** (Jun 2013)

52.237-3 **Continuity of Services** (Jan 1991)

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

52.203-17 **Contractor Employee Whistleblower Rights and Requirement To Inform Employees of Whistleblower Rights** (Apr 2014)

52.227-14 **Rights in Data** (May 2014)

52.245-1 **Government Property** (Jan 2017)

52.239-1 **Privacy or Security Safeguards** (Aug 1996)

52.232-40 **Providing Accelerated Payments to Small Business Subcontractors**(Dec 2013)

FAR clauses incorporated in full text

52.217-9 **Option to Extend the Term of the Contract** (Mar 2000)

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

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

(c)The total duration of this contract, including the exercise of any options under this clause, shall not exceed **48 months**.

HSAR clauses incorporated in full text

3052.204-71 – **Contractor Employee Access** (Sept 2012)

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

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

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

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

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

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

(c) Contractor employees working on this contract must complete such forms as may be necessary for security or other reasons, including the conduct of background investigations to determine suitability. Completed forms shall be submitted as directed by the Contracting Officer. Upon the Contracting Officer's request, the Contractor's employees shall be fingerprinted, or subject to other investigations as required. All Contractor employees requiring recurring access to Government facilities or access to sensitive information or IT resources are required to have a favorably adjudicated background investigation prior to commencing work on this contract unless this requirement is waived under Departmental procedures.

(d) The Contracting Officer may require the Contractor to prohibit individuals from working on the contract if the Government deems their initial or continued employment contrary to the

public interest for any reason, including, but not limited to, carelessness, insubordination, incompetence, or security concerns.

(e) Work under this contract may involve access to sensitive information. Therefore, the Contractor shall not disclose, orally or in writing, any sensitive information to any person unless authorized in writing by the Contracting Officer. For those Contractor employees authorized access to sensitive information, the Contractor shall ensure that these persons receive training concerning the protection and disclosure of sensitive information both during and after contract performance.

(f) The Contractor shall include the substance of this clause in all subcontracts at any tier where the subcontractor may have access tprivacy o Government facilities, sensitive information, or resources.

(End of clause)

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

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

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

The Key Personnel under this Contract are:

Project Manager, Level III [redacted]
Technical PM, Level II [redacted]

(End of clause)

Other Task Order Requirements

ADDITIONAL INVOICING INSTRUCTIONS

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

(1) Name and address of the contractor.

(2) Invoice date and invoice number.

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

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

(5) Shipping and payment terms.

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

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

(8) Taxpayer Identification Number (TIN).

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

(c) USCIS' preferred method for invoice submission is electronically. Invoices shall be submitted in Adobe pdf format with each pdf file containing only one invoice. The pdf files shall be submitted electronically to **USCISInvoice.Consolidation@ice.dhs.gov** with each email conforming to a size limit of 500 KB.

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

USCIS Invoice Consolidation
PO Box 1000
Williston, VT 05495

PERFORMANCE REPORTING

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

FINAL PAYMENT

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

GOVERNMENT-FURNISHED PROPERTY

(a) Upon the Contractor's request that a Contractor employee be granted access to a Government automated system and the Government's approval of the request, the Government will issue equipment to that employee by hand receipt: Laptop/Cell phone

(b) The Government may issue equipment to specified contractor employees.

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

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

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

Government Furnished Property	GFP will be furnished	GFP will be returned
Laptop (41 FTE's) (as duties require) ($2,500 EA)	EOD	Task Order Completion
Smartphone, (2) Key Personnel (as duties require) ($500 EA)	EOD	Task Order Completion

NOTICE TO PROCEED (NTP)

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

(b) The Contractor is responsible for submitting packages for employees who will receive favorable Entry-On-Duty (EOD) decisions and suitability determinations, and for submitting them in a timely manner. USCIS EOD process takes approximately 60 calendar days from a receipt of complete EOD packages. A Government decision not to grant a favorable EOD decision or suitability determination, or to later withdraw or terminate such, shall not excuse the Contractor from performance of its obligations under these task orders.

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

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

(e) The Government intends for the transition CLIN to begin once the contractor has successful obtained a suitability clearance. The contracting officer will issue a phase-in notice to proceed (NTP) once the contractor has EOD at least four (4) FTE's, two (2) of which must be the Project Manger positions under the Key Personnel section 7.2 of the PWS. This notice will be given at least one day before transition is to begin.

(f) The transition period shall last for 60 days. Successful completion of the transition period shall occur prior to any notice to proceed with full performance. The contracting officer will issue a full performance NTP once 41 FTE's have EOD. The notice will be given at least one day before full performance is to begin.

POSTING OF CONTRACT (OR ORDER) IN FOIA READING ROOM

(a) The Government intends to post the contract (or order) resulting from this solicitation to a public FOIA reading room.

(b) Within 30 days of award, the Contractor shall submit a redacted copy of the executed contract (or order) (including all attachments) suitable for public posting under the provisions of the Freedom of Information Act (FOIA). The Contractor shall submit the documents to the USCIS FOIA Office by email at **foiaerr.nrc@uscis.dhs.gov** with a courtesy copy to the contracting officer.

(c) The USCIS FOIA Office will notify the contractor of any disagreements with the Contractor's redactions before public posting of the contract or order in a public FOIA reading room.

Section D—List of Attachments

Attachment - Title	Pages
Performance Work Statement	24
Security Requirements	8
Safeguarding of Sensitive Information (MAR 2015)	9
Information Technology Security and Privacy Training (MAR 2015)	2
Accessibility Requirements (Section 508)	2
Labor Mix Table	1

United States Citizenship and Immigration Services

Performance Work Statement

IDENTITY, CREDENTIAL, and ACCESS MANAGEMENT - UNIFIED SERVICES (ICAM-US)

Contents

1. Overview

As a leader in the Federal Government's move to more Agile Development and Deployment models, the United States Citizenship and Immigration Services (USCIS) looks to transform all of its programs to more mature, effective, responsive and flexible DevOps models.

The USCIS Identity, Credential and Access Management (ICAM) Program award seeks to bring USCIS ICAM into that proven development culture by finding contractors who will structure deployment strategies such as Kanban/Scrum/Scrumban and organize teams to support "cradle to grave" development and deployment. The ICAM Program staff will seek to work with its different stakeholders within and outside the USCIS environment to bring them into the development, testing and Quality Assurance process in order to provide the highest quality solutions to its Government Business Owners and Immigrant customers.

2. Background

In November 2009, the Federal Chief Information Officers (CIO) Council released the Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance. ICAM consists of several traditionally segregated functional areas (Identity, Credential, Access and Federation) that, when managed collectively, provide security, privacy and process efficiency benefits that would not be achieved if managed individually. Most recently, OMB released M 11-11 (February 2011), which outlines specific ICAM-related requirements and delivery timelines for federal civilian agencies.

Due to the breadth and depth of the ICAM scope, a successful implementation will require multiple distinct projects—all of which must integrate across business and technology disciplines in order to achieve the expected outcomes. For this reason, a USCIS ICAM Program will be established to provide over-arching financial, business process and technical oversight to ensure ICAM mission success.

The USCIS ICAM Program will define, plan, promote, and coordinate the enterprise implementation of the USCIS ICAM environment in accordance with best practices. The ICAM Program staff will work with the different stakeholders within and outside the USCIS environment to determine existing initiatives and how they align to the ICAM Architecture and required functionality. The Program will be responsible for integrating all of the USCIS ICAM initiatives across the Agency through a common vision and strategy that will promote interoperability and reuse. It will do this through leveraging and integrating all Agency processes; including acquisitions, budgeting, security, engineering and architecture work streams.

Organizationally, the Program will be managed within the Office of the Chief Information Officer (OCIO) with strong collaboration from the Office of Security and Integrity (OSI) Specific project responsibilities will be mostly divided between OIT and OSI by the access control system type—Logical Access Control System (LACS) projects will be managed by OIT and Physical Access Control System (PACS) projects will be managed by OSI. As various teams from OIT and OSI work specific projects, the ICAM Program staff will ensure business and technology integration parity across all ICAM-related projects.

The program of consists of ten primary service areas:

- Identity Data Management
- Online Self Service
- Digital Workflow with Policy Enforcement

- Fully and Semi-automated Account Provisioning/De-provisioning
- Self-Service Password Management (allows for end-user password resets)
- Role, Policy or Attribute-based Authorization (depending on system type)
- Electronic Audit (all access-related actions stored in central DB)
- PIV Authentication (PACS and LACS)
- Reduced/Single Sign On
- Access Federation (PACS and LACS)

3. Objective

The objective of this Performance Work Statement (PWS) is to outline the technical/support requirements necessary to obtain the professional ICAM information technology services. These services include, but are not limited to, the design, architecture, engineering, documentation and maintenance of the enterprise implementation of the USCIS ICAM environment. Contractors will participate in team-based Agile environments that will be aligned in accordance with the ICAM Roadmap and Implementation guidance and USCIS Agile DevOps Development Methodologies, such the creation of a mature Continuous Integration/Continuous Delivery (CI/CD) model with a high level of automated testing integration.

4. Scope of Work

Given the specialized nature and urgency of this need, USCIS is seeking a contractor to provide ICAM information technology, systems engineering, and other professional services for the design, development, integration, testing, and delivery of incremental functional releases of the USCIS ICAM environment in accordance with the government-approved design and schedule. The contractor's testing processes shall confirm that the ICAM environment capabilities and services meet business expectations and performance specifications.

ICAM contractors are expected to provide high-performing, skilled development teams. Critical elements will be:

- High productivity
- High quality work
- Collaboration and cooperation with other teams and participants
- Technical skills and expertise as necessary
- Estimation and planning skills
- Innovation and creativity in problem solving

Scope:

- Validate and analyze requirements for the USCIS Enterprise ICAM environment and work with the assigned USCIS Product Owners to define them in user story format.
- Design, architect, engineer, and document the target Enterprise and Public ICAM environment and individual operational releases of that environment in an iterative fashion, focused on defining the minimum architectural components to which the program must adhere, then defining solution architectures at the release level.
- Design, develop, and maintain ICAM Identity proofing system.
- Develop and maintain custom software as components of the environment in an iterative fashion.

- Configure Government-furnished equipment (GFE) such as, but not limited to, Java-based identity and access management suites, including products from IBM, Oracle, Forge Rock and Mainframe solutions.
- Integrate GFE and other commercial and custom-developed software and GFE hardware components to create functional, operational releases of enterprise, Public ICAM services that continuously satisfies all USCIS, DHS, and federal ICAM requirements.
- Develop, maintain, and support USCIS use of utility software and processes needed to integrate with, consume and continuously reconcile ICAM-related data.
- Support the deployment of completed releases of the ICAM environment into production at DHS Data Centers and into USCIS administered Cloud environments; and into use for physical access control at facilities and logical access control over USCIS information networks, services and facilities.
- Assist and advise USCIS government and contract application developers and application maintenance staff to prepare applications for interoperation with the ICAM environment.

4.1 TECHNICAL LANDSCAPE

The contractor shall use DHS/USCIS development and test environments, including the public cloud.

The USCIS technical landscape is shifting from a proprietary Commercial Off The Shelf (COTS)-based framework to open source. USCIS has demonstrated success with a stack of predominately open source development and test tools that are currently under consideration for standardization across development teams. The ICAM contractor shall utilize such a standardized development and test suite, with the expectation that the development and test architecture will evolve.

The COTS and open source tools, languages, utilities, and applications currently used and under consideration for the standardized environment are identified in *Table 1: Current Test and Development Tool Suite*.

In addition to the toolsets listed in *Table 1: Current Test and Development Tool Suite*, ICAM developers under Legacy Integration Task Area will need to become familiar with and adapt to the specific software requirements of existing USCIS legacy applications for the purposes of Single Sign On integration as well as ICAM Authorization (AuthZ) development.

Name	Version	Manufacturer	Function
Test Tools (not limited to)			
Amazon Web Services		Amazon	Cloud computing services
AngularJS		AngularJS	Javascript Framework
Chef	0.1	Opscode	Open source software deployment
Confluence		Atlassian	Documentation Wiki
TPX			Mainframe Application
IDM Tool			Open IDM management

Name	Version	Manufacturer	Function
Docker		Docker Inc	Software containerization and deployment
Eclipse	Indigo sr2	Eclipse	IDE for software development
Git	1.7.10	Apache	Distributed version control
GitHub Enterprise		GitHub	Hosted code management
Gradle	1.0rc3	Gradle.org	Open source build automation tool
Hibernate	4	JBoss	Open source object / relational mapping library for Java
Java	1.8	Oracle	Language for software development
Jira		Atlassian	COTS ALM tool
JBoss Application Server	7.0.2	JBoss	Open source application server
JBoss Rules Engine	5	JBoss	Open source rules engine
Jenkins	1.4	Jenkins CI	Open source continuous integration server
Junit			Unit testing
Nexus	2.1	Sonatype	Open source repository manager
OpenAm		ForgeRock	Open source Access Management
OpenDJ		ForgeRock	Open Source LDAP
Oracle Database	11gR2	Oracle	Commercial database
Slack		Slack	Collaboration tool
Selenium			Browser testing in Firefox
Spring Framework	3.1.0e3.8	SpringSource.org	Open source Java framework
Development Tools (not limited to)			
Visual Studio Community	2015	Microsoft	Development IDE
Apache Directory Studio		Apache	LDAP browser and directory client
Active Directory RSAT		Microsoft	Active Directory Role Manager

Name	Version	Manufacturer	Function
Ruby/Ruby on Rails		Ruby	Open Source Web Application Framework

Table 1: Current Test and Development Tool Suite

5. Description of Requirements

The contractor shall provide all of the requirements described in the PWS necessary to perform the four ICAM tasks and two optional tasks as discussed in the subsections that follow. The contractor shall provide quality control management, Privacy Act compliance support, and contractor technical document quality reviews as indicated in the subsections that follow.

The contractor shall assist the ICAM Program Office in reaching out to oversight organizations, DHS and USCIS executives and managers, internal USCIS users, and external immigration mission customers to keep them informed of significant ICAM Program events that may impact their access to information systems or facilities.

All contractor-prepared communication materials and messages shall be coordinated and approved by the ICAM Program Manager and conveyed using broad, understandable language that highlights beneficial outcomes of ICAM Program activities and events.

Each subsection below provides specific details of ICAM work assignments, documentation, applicable standards, etc. and, in some cases, specifies required deliverables.

The contractor must be flexible to the DevOps model within USCIS which includes operation and development engineers participating together in the entire lifecycle, from design through the development process to production support. The contractor's approach to performing the described work shall be designed to promote and support the following Agile principles:

1. Early and continual user involvement
2. Frequent releases of end-to-end capabilities
3. Multiple, rapidly executed iterations that produce functionality to users for feedback no later than every two weeks
4. Early, successive delivery of functional product, or prototyping where functional product cannot be delivered
5. Automated implementation of build, deploy, test and release process (AKA: Deployment Pipeline. See Figure 1)
6. Modular, open systems approach (MOSA)
7. Organization of requirements into user stories that are Independent, Negotiable, Valuable, Estimable, Small and Testable (INVEST)

Figure 1. Continuous Deployment Pipeline Example[1]

Additionally, Section 6 of this PWS specifies knowledge and experience qualifications for all ICAM contractor staff that will be providing the services and support for the tasks described in this PWS, with additional qualifications stated for Key Personnel.

6. Tasks

The tasks identified in the following sections describe the work that will occur in order to accomplish the vision, as identified in Section 4. USCIS ICAM contractors shall provide teams that are able to perform the tasks as described, while conforming with the expectations outlined above, and with expert level ability in the technologies stated in section 4.1.

The contractor shall provide Agile DevOps teams for the purpose of responding to specific application development requirements USCIS ICAM identifies. The contractor's work shall conform to the architecture and design provided by the USCIS Architecture and Design team and the Agile processes set up by the USCIS Processes and Practices team.

Additionally, the contractor shall provide Agile DevOps teams capable of deploying code to a DHS Data Center as well as AWS public cloud. The contractor shall partner with IT and business stakeholders to ensure that software runs according to business requirements. The contractor shall support and deliver practical processes and foster collaboration between development and IT operations. The contractor will be working in DevOps-mode and shall be proactive in monitoring as well as reactive to alerts. Under the DevOps model, developers shall continue to have responsibility for the code even after it goes to production. Developers shall participate in the delivery of the code from creation to running in the pipeline to deployment and then maintenance.

Lastly, the teams provided in accordance with the Task Areas noted below shall, at all times shall include seven (7) FTE information technology professionals, except for the Management Task Area (Task Area 4) which shall consist of two (2) and the Legacy Integration Task Area (Task Area 3) which shall consist of four (4) . The contractor's commitment is to provide fully-staffed, fully functional teams. The skills of the team members must evolve over time as the technical landscape evolves. An individual will only serve on a team when that person's skills match the needed work.

6.1 TASK AREA 1 - ADMINISTRATIVE TASK AREA

This task area is to comprise one (1) team of two (2) administrative/technical assets. The contractor shall assign experienced personnel for program management and project planning. The contractor's resources shall possess knowledge and experience with program and project management, and administrative skills for this functional area.

a) The contractor shall collaborate with stakeholders, other support contractors, and third party vendors throughout system integration, performance, security, Section 508, system acceptance, user acceptance, usability, and test and evaluation reporting.
b) The contractor shall provide advice on commercial-off-the-shelf (COTS) and open source ICAM products, new platforms, and new ICAM technology solutions
c) The contractor shall manage all contractor resources and supervise all contractor staff in the performance of work on this task order. The contractor shall manage and

[1] Continuous Delivery: Reliable Software Releases through Build, Test, and Deployment Automation; by Jez Humble and David Farley; ISBN 9780321601919; August 2010; Addison-Wesley

coordinate its team(s) on a day-to-day basis and ensure plans are communicated to team members. Likewise, the contractor must ensure that the health and progress against those plans are adequately reported.

d) The contractor shall organize, direct and coordinate administrative and technical planning as well as execution of all task order activities.

e) Vehicles for transparency, such as but not limited to, the Application Lifecycle Management (ALM) tool JIRA, shall be maintained with data so that reports and charts can be generated as needed, and so that user stories, defects, and tasks and their status are available to stakeholders. Task boards and SharePoint sites, meetings, and demos can be used to share information and report progress.

f) The contractor shall create a Quality Management Plan.

g) The contractor shall ensure development-related activities are in accordance with the contractor's Quality Management Plan.

6.2 TASK AREA 2 - ICAM ENTERPRISE TASK AREA

This task area is to comprise four (4) teams of seven (7) technical assets that are charged with supporting and expanding on current ICAM functionality and features as well as maturing the ICAM Authentication (AuthN) and Authorization (AuthZ) methods. This Task Area also supports the remediation of existing/future security Plan of Action and Milestone (POA&M) items. In conjunction with AuthN efforts, USCIS is also leading the Federal Government's effort to have 100% full PIV card enablement for both Privileged as well as Non-Privileged users in all USCIS standard and Mainframe systems.

a) The contractor shall be responsible for delivery teams performing the full suite of delivery tasks using Agile methodologies, including, but not limited to: participating in creating user stories for both business functionality, technical requirements and defining acceptance criteria; estimating the size of stories; solution design; development; testing, infrastructure provisioning, operations, and security.

b) The contractor shall assist in the documentation of user stories, acceptance criteria and tasks to be completed to fulfill the definition of done for a story.

c) The contractor shall develop code and other artifacts against the user stories documented in task *6.2.a* or as assigned by the government.

d) The contractor shall provide traceability of all corrected defects back to the original User Story

e) The contractor shall regularly validate their user interface mockups and perform usability testing with system stakeholders; including subject matter experts, interface partners and regular users.

f) The contractor shall respond to production incidents, including but not limited to, breakages of functionality, system outages, and performance problems. This responsibility includes, but is not limited to, investigating and triaging incidents, rolling systems back to earlier states, developing and deploying fixes (on software they may or may not have developed), engaging with other contractors and federal employees to fix related systems, and running incident retrospectives to ensure permanent fixes and deliver status reports and after-action retrospectives to the USCIS ICAM PMO.

g) The contractor shall develop code that does not add new technical debt to a release; however, there may be instances where technical debt is unavoidable and may be incurred with the government's approval. In these cases, the contractor shall actively work to decrease technical debt; the contractor shall correct any defects identified by testers, code reviewers, automated tools, or as part of the CI/CD activities etc.

h) The contractor's work shall conform to the architecture and standards provided by the government and the Agile processes set up by the USCIS Processes and Practices team. This will include providing input to any documentation required to maintain compliance with DHS and USCIS standards, as specified by USCIS.

i) The contractor shall architect, develop, automate and deploy software in accordance with industry best practices. This includes, but is not limited to, following 12 Factor App development practices (12factor.net), building stateless microservices, and deploying software with zero downtime. The contractor shall stay fluent with industry best practices as they evolve.

j) The contractor's code shall meet the functional and non-functional requirements, meet database development requirements, meet testing requirements, and be deployable and fully tested.

k) The contractor shall ensure that defect corrections are fully tested before deployment.

l) The contractor shall provide integration support to USCIS Legacy Mainframe applications using COTS software, ensure the mainframe applications are PIV enabled, and provide O&M support for the mainframe applications

m) The contractor shall be knowledgeable in both Windows and Unix/Linux Operating Systems in order to integrate Mainframe applications and continuous O&M support.

n) Configure Government-furnished equipment (GFE) such as, but not limited to, Java-based identity and access management suites, including products from IBM, Oracle, Forge Rock and Mainframe solutions;

o) Integrate commercial and custom-developed software as well as GFE hardware components in USCIS Data Centers or USCIS administered public cloud as needed to create functional, operational releases of enterprise, Public ICAM services that continuously satisfies all USCIS, DHS, and federal ICAM requirements; develop, maintain, and support USCIS use of utility software and processes needed to integrate with, consume and continuously reconcile ICAM-related data;

p) Deploy completed releases of the ICAM environment into production at DHS Data Centers or USCIS administered public cloud and into use for physical access control at facilities and logical access control over USCIS information networks, services and facilities;

q) Assist and advise USCIS government and contract application developers and application maintenance staff to prepare applications for interoperation with the ICAM environment;

r) Provide continuous 24 X 7 operational support for the ICAM Enterprise environments.

s) Assist with overall ICAM environments and/or release coordination, scheduling, and collaboration with other USCIS IT projects and with external stakeholder organizations that require access to USCIS facilities and information resources

t) Support reviews of technical documents developed external to the ICAM Program and that reference or document use of ICAM services, or that provide services required by the ICAM environment

u) Analyze and report on special ICAM and Agile & continuous delivery topics and best practices specific to the ICAM environment as requested

v) Apply the principles of DevOps as part of overall integrated Agile practices.

w) Document meetings, including action, risk, and issues items

x) Provide support for the ICAM Program Manager, ICAM Product Owner and the Executive Steering Committee (ESC) when planning and conducting ICAM Program meetings

y) Provide the ICAM Program Manager and ICAM Product Owner with executive level briefing materials, including talking points, illustrative diagrams, and flowcharts

z) Track open impediments, action items, Change requests and other program management related documents

aa) Ensure use of USCIS Office of Information Technology (OIT) standard enterprise planning and tracking tools. The contractor shall utilize processes that ensure continuity of operations and smooth transition of the management responsibilities throughout the life of the contract

bb) The contractor shall design and develop solutions that conform to the federal ICAM segment architecture. Lead engineers (or architects) shall provide for the execution of continuous delivery of USCIS ICAM releases into full operational status.

cc) The contractor shall augment and tailor the USCIS identity and access management solutions using commercial, open source, and custom-developed software, as required. The contractor shall deploy and maintain all other software, hosting, data, and configuration elements of the USCIS ICAM environments.

dd) The contractor shall provide support to the ICAM system architecture planning efforts including the Performance, Business, Data, and System Architectures consistent with DHS Enterprise Architecture (EA) guidelines. This task shall include but is not limited to engaging stakeholders, coordinating with other Government Integrated Product Teams (IPTs), and participating in teams and task forces in support of the Architecture IPT Lead

ee) Support the evolution of the Target (To-Be) Architecture. This includes providing subject matter expert support to design and recommending target architectures. This includes providing descriptions and illustrations of the target environments for all architectural components such as business, data/information, technology, etc.

ff) Support the development of transition plans and the system roadmap. This includes providing subject matter expert support to develop plans for transitioning from the Baseline to the Target Architecture, including transition strategies; strategic plans; sequencing plans; investment portfolio analysis, impact analyses; dependency diagrams; roadmaps

gg) Support the evaluation of implementation results. This includes evaluating progress and results of projects to examine compliance with the USCIS Architecture, result effectiveness, and execution efficiency; analyzing problems; making recommendations

hh) Support the Enterprise Architecture Board (EAB) and Enterprise Architecture Center of Excellence (EACOE) and approval process

6.3 TASK AREA 3 - ICAM PUBLIC TASK AREA

This task area is to comprise one (1) team of seven (7) technical assets that are charged with supporting and expanding on current public ICAM functionality and integration with the USCIS projects ELIS and IDPaaS. This Task Area also supports the remediation of existing/future security POAM items. In conjunction with current efforts, USCIS is also is exploring integration with the General Services Administration's 'Login.gov' project, which will provide public customers an eventual "One Stop" authentication to US Government services. The contractor team would be required to work interactively with diverse non-USCIS teams to integrate across components/departments/agencies.

a) The contractor shall be responsible for delivery teams performing the full suite of delivery tasks using Agile methodologies, including, but not limited to: participating in creating user stories for both business functionality, technical requirements and defining acceptance criteria; estimating the size of stories; solution design; development; testing, infrastructure provisioning, operations, and security.

b) The contractor shall assist in the documentation of user stories, acceptance criteria and tasks to be completed to fulfill the definition of done for a story.

c) The contractor shall develop code and other artifacts against the user stories documented in task *6.2.a* or as assigned by the government.

d) The contractor shall provide traceability of all corrected defects back to the original User Story

e) The contractor shall regularly validate their user interface mockups and perform usability testing with system stakeholders; including subject matter experts, interface partners and regular users.

f) The contractor shall respond to production incidents, including but not limited to, breakages of functionality, system outages, and performance problems. This responsibility includes, but is not limited to, investigating and triaging incidents, rolling systems back to earlier states, developing and deploying fixes (on software they may or may not have developed), engaging with other contractors and federal employees to fix related systems, and running incident retrospectives to ensure permanent fixes and deliver status reports and after-action retrospectives to the USCIS ICAM PMO.

g) The contractor shall develop code that does not add new technical debt to a release; however, there may be instances where technical debt is unavoidable and may be incurred with the government's approval. In these cases, the contractor shall actively work to decrease technical debt; the contractor shall correct any defects identified by testers, code reviewers, automated tools, or as part of the CI/CD activities etc.

h) The contractor's work shall conform to the architecture and standards provided by the government and the Agile processes set up by the USCIS Processes and Practices team. This will include providing input to any documentation required to maintain compliance with DHS and USCIS standards, as specified by USCIS.

i) The contractor shall architect, develop, automate and deploy software in accordance with industry best practices. This includes, but is not limited to, following 12 Factor App development practices (12factor.net), building stateless microservices, and deploying software with zero downtime. The contractor shall stay fluent with industry best practices as they evolve.

j) The contractor's code shall meet the functional and non-functional requirements, meet database development requirements, meet testing requirements, and be deployable and fully tested.

k) The contractor shall ensure that defect corrections are fully tested before deployment.

l) The contractor shall provide support to USCIS Legacy Mainframe systems, ensure the mainframe applications are PIV enabled and provide O&M support for the mainframe applications

m) Configure Government-furnished equipment (GFE) such as, but not limited to, Java-based identity and access management suites, including products from IBM, Oracle, Forge Rock and Mainframe solutions;

n) Integrate commercial and custom-developed software as well as GFE hardware components in USCIS Data Centers or USCIS administered public cloud as needed to create functional, operational releases of enterprise, Public ICAM services that continuously satisfies all USCIS, DHS, and federal ICAM requirements; Develop, maintain, and support USCIS use of utility software and processes needed to integrate with, consume and continuously reconcile ICAM-related data;

o) Deploy completed releases of the ICAM environment into production at DHS Data Centers or the USCIS administered public cloud and into use for physical access control at facilities and logical access control over USCIS information networks, services and facilities;

p) Assist and advise USCIS government and contract application developers and application maintenance staff to prepare applications for interoperation with the ICAM environment;

q) Provide continuous 24 X 7 operational support for the ICAM Public environments.

r) Assist with overall ICAM environments and/or release coordination, scheduling, and collaboration with other USCIS IT projects and with external stakeholder organizations that require access to USCIS facilities and information resources

s) Support reviews of technical documents developed external to the ICAM Program and that reference or document use of ICAM services, or that provide services required by the ICAM environment

t) Analyze and report on special ICAM and Agile & continuous delivery topics and best practices specific to the ICAM environment as requested

u) Apply the principles of DevOps as part of overall integrated Agile practices.

v) Document meetings, including action, risk, and issues items

w) Provide support for the ICAM Program Manager, ICAM Product Owner and the Executive Steering Committee (ESC) when planning and conducting ICAM Program meetings

x) Provide the ICAM Program Manager and ICAM Product Owner with executive level briefing materials, including talking points, illustrative diagrams, and flowcharts

y) Track open impediments, action items, Change requests and other program management related documents

z) Ensure use of USCIS Office of Information Technology (OIT) standard enterprise planning and tracking tools. The contractor shall utilize processes that ensure continuity of operations and smooth transition of the management responsibilities throughout the life of the contract

aa) The contractor shall design and develop solutions that conform to the federal ICAM segment architecture. Lead engineers (or architects) shall provide for the execution of continuous delivery of USCIS ICAM releases into full operational status.

bb) The contractor shall augment and tailor the USCIS identity and access management solutions using commercial, open source, and custom-developed software, as required. The contractor shall deploy and maintain all other software, hosting, data, and configuration elements of the USCIS ICAM environments.

cc) The contractor shall provide support to the ICAM system architecture planning efforts including the Performance, Business, Data, and System Architectures consistent with DHS Enterprise Architecture (EA) guidelines. This task shall include but is not limited to engaging stakeholders, coordinating with other Government Integrated Product Teams (IPTs), and participating in teams and task forces in support of the Architecture IPT Lead

dd) Support the evolution of the Target (To-Be) Architecture. This includes providing subject matter expert support to design and recommending target architectures. This includes providing descriptions and illustrations of the target environments for all architectural components such as business, data/information, technology, etc.

ee) Support the development of transition plans and the system roadmap. This includes providing subject matter expert support to develop plans for transitioning from the Baseline to the Target Architecture, including transition strategies; strategic plans; sequencing plans; investment portfolio analysis, impact analyses; dependency diagrams; roadmaps

ff) Support the evaluation of implementation results. This includes evaluating progress and results of projects to examine compliance with the USCIS Architecture, result effectiveness, and execution efficiency; analyzing problems; making recommendations

gg) Support the Enterprise Architecture Board (EAB) and Enterprise Architecture Center of Excellence (EACOE) and approval process

6.4 TASK AREA 4 - ICAM LEGACY INTEGRATION TASK AREA

This task area is to comprise one (1) team of four (4) technical assets that are charged with assisting in the integration of ICAM connection points with USCIS legacy applications.

The contractor shall provide support to USCIS projects that will implement PIV-based Single Sign-On (SSO) for authenticating user identities and controlling access to nearly all electronic services in the USCIS inventory, including desktop computing systems, networks, and applications, as well as managing access to USCIS and DHS facilities. This task shall include but is not be limited to:

- Assist and advise USCIS federal employees and other contractors to implement processes and procedures for maintaining and utilizing PIV Cards and PIV PKI certificates
- Deliver capabilities that support wide-spread PIV card usage for authentication to physical and logical access control systems, including but not limited to implementation of and support for: PKI certificate validation systems, PKI integration with operating system and application specific cryptographic application program interfaces and certificate stores, provisioning of PIV card and or PIV PKI attributes to associated relying systems, development, deployment and support for PIV "Service Stations" supporting functions such as PIN reset, PKI certificate updates, and activation of centrally printed PIV cards, and enrollment of PIV card and PIV PKI data into Physical Access Control Systems
- In conjunction with the ICAM Enterprise team, support the implementation of PIV-based authentication services for USCIS desktop computing systems, networks, and applications
- Plan and execute projects that will enable and facilitate transition from existing USCIS "soft" PKI certificates used for digital signatures and encryption to PIV-based smart card PKI certificates for usage with digital signatures, encryption and authentication
- In conjunction with the ICAM Enterprise team, assist in integrating USCIS physical access control systems with the USCIS identity management and access management services
- Assist in the implementation of ICAM derived technical solutions in USCIS legacy applications in support of SSO/PIV integration.

6.5 TASK AREA 5 – PHASE IN/OUT

The contractor shall be responsible for the transition of all technical activities identified in this PWS. The technical activities, which shall be included as part of the phase-in (also referred to as 'transition-in'), consist of:

- Inventory and orderly transfer of all Government Furnished Property, software and licenses
- Transfer of documentation currently in process
- Transfer of all software coding in process
- Coordinating the body of work with the current contractor

The contractor's Transition-In Plan shall be approved by USCIS OIT and shall contain a milestone schedule of events and system turnovers. The Transition-In Plan shall address transition of systems with no disruption in operational services. To ensure the necessary continuity of services and to maintain the current level of support, the Government may retain services of the incumbent contractor for some or all of the phase-in period and up to 30 days of the Base period, as may be required.

For the Transition-In Plan, the contractor shall include its staffing ramp-up approach and ensure that all FTEs billed on the task order are fully engaged in USCIS work and have received clearance(s)/badge(s).

At a minimum, the contractor's plan shall include its innovative and proactive approach to manage the following transition activities with the incumbent contractor and/or the Government:

- Assuming responsibility for current support services,
- Assuming ownership of historic data, documentation, processes, training, and tools
- Assuming user and system administration for all systems and tools
- Transferring assets
- Accepting the transfer of all compiled and un-compiled source code (all versions, updates, and patches)

- Obtaining access (keys, cards, security codes) and required training
- Conducting introduction/orientation activities

The contractor shall include its approach to provide analyses, validations, updates, and recommendations for enhancement to include, at a minimum:

- Inventory validation within 20 days after transition conclusion
- Plans and system analysis and update within 30 days after transition conclusion
- Other documentation analysis and update within 30 days after transition conclusion

The Transition-Out Plan shall describe all required transition-out activities necessary to ensure a successful and timely transition to a successor (either a Government entity, another contractor, or to the incumbent contractor under a new contract/order). The Transition-Out Plan shall also include a project schedule based on days prior to contract expiration by which the contractor will execute the activities described in the Transition-Out Plan in coordination with the Government and the successor. The Transition-Out Plan should allow for no more than 30 days for completion of transition activities to the successor.

In keeping with accepted Lean Practice, USCIS seeks to automate the Phase In/Phase Out processes to the greatest extent possible, relying less on traditional paper or electronic documentation.

7. Required staffing Expertise and Experience, Key Personnel

The Contractor shall staff the ICAM contract with highly skilled and experienced personnel resources, as described below, to perform the task areas outlined in this Performance Work Statement.

All Contractor personnel working on this contract, for the duration of this contract, shall comply with the DHS/USCIS Security Requirements Attached to this PWS. The Contractor shall appoint a senior official to act as the Corporate Security Office. 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 "Security's Requirements" are outlined in Attachment 2.

7.1 Labor Categories

The advanced experience of the ICAM contractor staff is directly related to the successful outcome of the ICAM Program. The contractor shall provide professional technical personnel with proven ICAM program management and technical leadership skills, as well as engineers and other technical experts with in-depth technical knowledge and hands-on experience with Java-based identity and access management suites, including products from IBM, Oracle, mainframe, and ForgeRock. Experience in solutions development where Agile Development principles were successfully applied is highly desirable. This level of experience and technical knowledge of ICAM products is essential to plan and execute the planning, engineering, development, integration, and deployment of the USCIS enterprise ICAM environment.

7.2 Key Personnel and Other Experience Requirements

Key Personnel are critical to the success of this work and shall meet the experience and other requirements set forth in the paragraph below.

Contractor shall provide a statement of qualifications for proposed key personnel within 10 days following award that identifies certification, type and extent of experience and ICAM-related

knowledge to show proposed key personnel meets or exceeds the requirements of the solicitation. USCIS Program Manager shall accept or reject proposed key personnel within 5 days.

- The Project Manager shall have at least five years of experience as a Lead Engineer in an ICAM-related environment, and at least five years of experience of domain knowledge in ICAM, managing large complex, mission critical web-based systems development projects and programs
- The Project Manager must have in-depth knowledge of federal ICAM standards and the *Federal ICAM Roadmap and Implementation Guidance*, as well as knowledge of the capabilities, strengths, and weaknesses of current commercial and open-source ICAM products

The CO must approve all changes in Key Personnel. Prior to changes in Key Personnel, the Contractor shall notify the CO via the COR reasonably in advance (not less than 15 days prior) and shall submit a justification (including proposed substitutions) in sufficient detail to permit evaluation of the impact of this change to the task order.

The replacement shall possess qualifications equal or superior to those of the previous personnel occupying the Key or Essential position. The Contractor shall ensure knowledge transfer and full transition of responsibilities occurs, without the Government having to request the transfer and without further cost to the Government, between the Key or Essential person and the replacement. Before removing or replacing any of the specified individuals (for other than cause), the Contractor shall notify the Contracting Officer, in writing, before the change becomes effective. When a specified individual requires removal or replacement for cause, the Contractor shall notify the Contracting Officer. The Contractor shall submit sufficient information to the Contracting Officer to evaluate the potential impact of the change on this task order.

8. Deliverables and Delivery Schedule

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

8.1 TABLE: DELIVERABLES SCHEDULE

ITEM	FREQUENCY OF DELIVERY	ACCEPTABLE FORMATS
Statement of qualifications for proposed key personnel	With 10 days of Task Order Award	MS Word 2010
In-process application code	Continuously, with each build	Application source code
Shippable application code	Continuously, with each commit	Application source code and compiled code
Quality Control Plan	30 days After Receipt of Order (ARO) Updated annually	MS Word 2010

Quarterly Project Management Review	Quarterly	MS Word 2010
Agile development lifecycle documents, such as System Design Document (SDD), etc.	Each release	MS Word 2010
Status Briefings, such as presentations, database extractions, meeting reports, burndown charts, etc.	Weekly	MS Word 2010, Excel, Visio, or PowerPoint
Transition Plan In / Out	60 days prior to either Transition In or Transition Out.	MS Word 2010
Security Plan	Updated as needed to include Security profile/boundaries changes.	MS Word 2010
Test Scripts	Continuously, with each commit	Application source code, MS Word 2010
Corporate Telework Plan	As Directed	MS Word 2010
Separation Notification (Attachment 2)	Within 5 days of each occurrence	As directed
Separation Notification	The CO and COR must be notified of each contract employee termination/resignation. (The COR will then notify the Office of Security & Integrity (OSI) Personnel Security Division (PSD) to coordinate the exit clearance forms.	Within five (5) days of each occurrence.

8.2 DELIVERABLE ACCEPTANCE CRITERIA

Deliverables shall be submitted to the Contracting Officer and COR, or, as in the case of application code, uploaded to the USCIS GitHub code repository for CO/COR acceptance. The COR will notify the contractor of final deliverable acceptance or provide comments in writing within ten (10) business days of receipt. Contractor shall make the necessary changes to the final deliverable and re-submit within 15 business days to the COR and Contracting Officer, if necessary, for final acceptance. Specific acceptance criteria will be identified with each user storyboard.

All deliverables shall be delivered without proprietary markings and shall be delivered with unlimited rights as per FAR 52.227-17.

9. Place of Performance/Hours of Operation

The principal place of performance shall be at the USCIS Main Headquarters locations, in, Washington, DC. Meetings will usually take place at USCIS offices in the Washington, DC Metropolitan Area.

9.1 TELEWORK

Episodic Telework is authorized in support of this effort. In addition, Telework is authorized in support of this effort based on the contractor's telework guidance after review and acceptance of the Contractor's Corporate Telework Plan by the Contracting Officer. The Contractor's Corporate Telework Plan is due at the kick-off meeting. Before beginning to telework, all employees shall complete the annual Computer Security Awareness Training (CSAT) requirement, access to which shall be provided by USCIS.

Telework shall be considered a privilege, not a right, and shall not impact contractor's productivity and participation in any agile sessions or government meetings.

9.2 HOURS OF OPERATION

The ICAM Program Office is located at USCIS Headquarters, 111 Massachusetts Ave NW, Washington, DC 20001. The ICAM Program currently operates Monday – Friday during core business hours, excluding Federal Holidays. The core business hours are 8:00AM – 5:30 PM. At times, based on the needs of the mission, the Government will require service outside of the normal duty hours and upon COR/PM direction, and given an advanced notice if possible, the contractor shall work weekends and Government holidays. USCIS Government employees must be present during such instances. The contractor shall be available during this time period.

9.3 GOVERNMENT HOLIDAYS

Government holidays are noted below. When federal offices are closed for holiday or any reason, the contractor shall comply with OPM's operating status. Contractor shall not invoice for days when federal offices are closed for holiday or any reason.

Month	Holiday
January	New Year's Day Martin Luther's King Day
February	President's Day
May	Memorial Day
July	Independence Day
September	Labor Day

October	Columbus Day
November	Veteran's Day Thanksgiving Day
December	Christmas Day

10. Government Furnished Property (GFP) / Information (GFI)

Only GFP laptops 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. A webinar account, such as AT&T Connect, Adobe Connect will be provided to the contractor to facilitate virtual demos and other meetings with stakeholders at various physical locations. Smartphone devices may be provided as identified by the COR or Government Program Manager.

The Government has the right to implement Workplace as a Service (WPaaS) in lieu of providing GFP or as a replacement for existing GFP at its discretion during the life of the contract.

A list of GFP will be incorporated into the task order.

11. Travel

No travel is anticipated.

12. Performance Measures and Acceptance Criteria

Performance Standards. The contractor service requirements are summarized into performance objectives that relate directly to mission essential items. The performance standards describe the acceptable level of performance required for each performance objective. These standards are critical to mission success and are identified in the table below:

Indicators/Tasks	**PWS Section**	**AQL Performance Standard**	**Monitoring Method**
Management Oversight/Responsiveness	6 and 7	Contractor maintains open lines of communication and it is responsive to performance concerns that may have a negligible adverse impact to the customer's mission support and readiness.	Continuous Monitoring
ICAM Design, oversight, and Testing Services	5,6 and 8	100% in compliance with applicable documents and standards	Implementation Schedule and Quarterly Reviews
PIV & PKI	6.2,6.3 and 6.4	100% in compliance with applicable documents and standards per USCIS and DHS	Implementation Schedule, Quarterly, Annual Reviews

Indicators/Tasks	**PWS Section**	**AQL Performance Standard**	**Monitoring Method**
Security	6 and 7	Meet DHS and USCIS security requirements, with no adverse effect on performance, with 100% compliance	Random Inspection
Process Quality and Assurance	6.1 and 8	Daily Standups, Demos. Retrospectives, with 95% compliance	Continuous Inspection, Implementation Schedule, Rally (Tool), Quarterly, Annually, Daily
ICAM Development, implementation, operation and maintenance.	6 and 8	100% in compliance with applicable documents and standards	Implementation Schedule and Quarterly Reviews
ICAM Data Management Services	6 and 8	95% successful transition of data in appropriate ICAM environment	Implementation Schedule, Quarterly, Annual Reviews
Deliverables	8	99% of the time deliverables are provided within required timeframe	Continuous Inspection
Cycle Time	5, 6	Time spent working on an issue: as in the time taken from when work begins on an issue to when work is completed. Cycle time also includes any other time spent working on the issue (eg. Reopening an issue, reworking it and closing it out again)	Jira ALM tool, GitHub reports - Daily
Code Quality and Standards	5, 6	Based on Automated Function Points (AFP) and/or Automated Quality Characteristic Measures to enable software quality and productivity analysis, cost and estimation factoring.	Jira ALM tool, GitHub reports – Daily

Indicators/Tasks	PWS Section	AQL Performance Standard	Monitoring Method
Business Satisfaction and Value	5, 6	Based on Program and Business owner feedback. Value determination consists of feature significance, usage and availability, and functionality assessment data collected through survey analysis.	Daily Standups, Sprint grooming, retrospectives, Business surveys, - Daily/Weekly/Monthly

Government Surveillance: Government surveillance of the contractor's performance shall include periodic government inspections at the performance locations and review of the deliverables.

Remedies: The government reserves the right to negotiate consideration for continued failures to meet performance standards. This does not include performance failures due to circumstances beyond the contractor's control.

13. DHS Enterprise Architecture Compliance

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

- All developed solutions and requirements shall be compliant with the HLS and USCIS EA and governance processes.
- All IT hardware and/or software shall be compliant with the DHS and USCIS EA Technical Reference Model (TRM) Standards and Products Profile.
- All data assets, information exchanges and data standards, whether adopted or developed, shall be submitted to the Enterprise Data Management Office (EDMO) for review and insertion into the DHS and USCIS Data Reference Model.
- In compliance with Office of Management & Budget (OMB) mandates, all network hardware shall be IPv6 compatible without modification, upgrade, or replacement.
- All service assets, WSDL, service exchanges and standards, whether adopted or developed shall be submitted to the USCIS EA for review and inserted into the USCIS and DHS Service Reference Model.
- All performance assets whether adopted or developed shall be submitted to the USCIS EA for review and insertion into the USCIS performance architecture.

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

14.1 BACKGROUND

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

14.2 REQUIREMENT

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

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

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

The contractor shall, after OIT's determination on whether or not the release meets the capitalization criteria, support OIT's reporting of costs incurred for the project or release, as required. The contractor shall provide the nature and cost of work completed within the relevant period. Costs considered part of IUS activities include systems administration, systems engineering, and program management. The Contractor shall provide the total cost, itemized by release and include the total sum of all applicable IUS activities. This information shall be submitted as outlined in the deliverables schedule. Excel spreadsheets will be provided after award. For information purposes, the following activities within the development lifecycle have been identified as IUS reportable costs by the USCIS Management Directive No. 128-001:

a) Design: System Design: Design System, Update System Test Plan, Update Security Test Plan, Update Project Plan, Update Business Case, Conduct Critical Design Review and Issue Memo.
b) Programming/Construction: Establish Development Environment, Create or Modify Programs, Conduct Unit & Integration Testing, Develop Operator's Manual, Update Project Plan, Update Business Case, Migration Turnover/Test Readiness Review, Prepare Turnover Package, Develop Test Plans, Migration Turnover/Issue Test Readiness Memo
c) Testing

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

ii. Coding

iii. Installation to hardware

iv. Testing, including parallel processing phase

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

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

Ref: (a) USCIS Management Directive No. 128-001

(b) Federal Accounting Standards Advisory Board Handbook, Standard 10, Accounting for Internal Use Software

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

SECURITY REQUIREMENTS

GENERAL

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

SUITABILITY DETERMINATION

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

BACKGROUND INVESTIGATIONS

Contractor employees (to include applicants, temporaries, part-time and replacement employees) under the contract, needing access to sensitive but unclassified information shall undergo a position sensitivity analysis based on the duties each individual will perform on the contract as outlined in the Position Designation Determination (PDD) for Contractor Personnel. The results of the position sensitivity analysis shall identify the appropriate background investigation to be conducted. All background investigations will be processed through OSI PSD.

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

Completed packages must be submitted to OSI PSD for prospective Contractor employees no less than 30 days before the starting date of the contract or 30 days prior to EOD of any employees, whether a replacement, addition, subcontractor employee, or vendor. The Contractor shall follow guidelines for package submission as set forth by OSI PSD. A complete package will include the

following forms, in conjunction with security questionnaire submission of the SF-85P, "Security Questionnaire for Public Trust Positions" via e-QIP:

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

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

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

4. Position Designation Determination for Contract Personnel Form

5. Foreign National Relatives or Associates Statement

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

7. ER-856, "Contract Employee Code Sheet"

EMPLOYMENT ELIGIBILITY

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

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

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

CONTINUED ELIGIBILITY

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

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

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

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

- **USCIS Security Awareness Training** (required within 30 days of entry on duty for new contractors, and annually thereafter)
- **USCIS Integrity Training** (Annually)
- **DHS Continuity of Operations Awareness Training** (one-time training for contractors identified as providing an essential service)
- **USCIS Office Safety Training** (one-time training for contractors working within USCIS facilities; contractor companies may substitute their own training)
- **USCIS Fire Prevention and Safety Training** (one-time training for contractors working within USCIS facilities; contractor companies may substitute their own training)

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

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

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

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

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

Contractor employees who do not have a PIV card must schedule an appointment to have one issued. To schedule an appointment:
http://ecn.uscis.dhs.gov/team/mgmt/Offices/osi/FSD/HSPD12/PIV/default.aspx
Contractors who are unable to access the hyperlink above shall contact the Contracting Officer's Representative (COR) for assistance.

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

A contractor employee required to have a PIV card shall:

- Properly display the PIV card above the waist and below the neck with the photo facing out so that it is visible at all times while in a USCIS facility
- Keep their PIV card current
- Properly store the PIV card while not in use to prevent against loss or theft
  http://ecn.uscis.dhs.gov/team/mgmt/Offices/osi/FSD/HSPD12/SIR/default.aspx

OSI PSD must be notified of all terminations/ resignations within five days of occurrence. The Contractor will return any expired USCIS issued identification cards and HSPD-12 card, or those of terminated employees to the COR. If an identification card or HSPD-12 card is not available to be returned, a report must be submitted to the COR, referencing the card number, name of individual to whom issued, the last known location and disposition of the card.

SECURITY MANAGEMENT

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

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

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

SECURITY PROGRAM BACKGROUND

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

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

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

GENERAL

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

IT SYSTEMS SECURITY

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

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

IT SECURITY IN THE SYSTEMS DEVELOPMENT LIFE CYCLE (SDLC)

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

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

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

SECURITY ASSURANCES

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

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

DATA SECURITY

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

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

SAFEGUARDING OF SENSITIVE INFORMATION (MAR 2015)

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

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

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

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

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

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

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

the Department of Homeland Security (including the Assistant Secretary for the Transportation Security Administration or his/her designee);

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

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

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

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

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

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

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

(1) DHS Management Directive 11042.1 Safeguarding Sensitive But Unclassified (for Official Use Only) Information

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

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

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

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

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

(4) The Contractor's invoicing, billing, and other recordkeeping systems maintained to support financial or other administrative functions shall not maintain SPII. It is acceptable to maintain in

these systems the names, titles and contact information for the COR or other Government personnel associated with the administration of the contract, as needed.

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

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

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

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

(iii) Support the completion of the Privacy Threshold Analysis (PTA) as needed. As part of the SA process, the Contractor may be required to support the Government in the completion of the PTA. The requirement to complete a PTA is triggered by the creation, use, modification, upgrade, or disposition of a Contractor IT system that will store, maintain and use PII, and must be renewed at least every three (3) years. Upon review of the PTA, the DHS Privacy Office determines whether a Privacy Impact Assessment (PIA) and/or Privacy Act System of Records Notice (SORN), or modifications thereto, are required. The Contractor shall provide all support necessary to assist the Department in completing the PIA

in a timely manner and shall ensure that project management plans and schedules include time for the completion of the PTA, PIA, and SORN (to the extent required) as milestones. Support in this context includes responding timely to requests for information from the Government about the use, access, storage, and maintenance of PII on the Contractor's system, and providing timely review of relevant compliance documents for factual accuracy. Information on the DHS privacy compliance process, including PTAs, PIAs, and SORNs, is accessible at http://www.dhs.gov/privacy-compliance.

(2) *Renewal of ATO.* Unless otherwise specified in the ATO letter, the ATO shall be renewed every three (3) years. The Contractor is required to update its SA package as part of the ATO renewal process. The Contractor shall update its SA package by one of the following methods: (1) Updating the SA documentation in the DHS automated information assurance tool for acceptance by the Headquarters or Component CIO, or designee, at least 90 days before the ATO expiration date for review and verification of security controls; or (2) Submitting an updated SA package directly to the COR for approval by the Headquarters or Component CIO, or designee, at least 90 days before the ATO expiration date for review and verification of security controls. The 90 day review process is independent of the system production date and therefore it is important that the Contractor build the review into project schedules. The reviews may include onsite visits that involve physical or logical inspection of the Contractor environment to ensure controls are in place.

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

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

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

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

(f) *Sensitive Information Incident Reporting Requirements.*

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

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

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

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

(g) *Sensitive Information Incident Response Requirements.*

(1) All determinations related to sensitive information incidents, including response activities, notifications to affected individuals and/or Federal agencies, and related services (e.g., credit monitoring) will be made in writing by the Contracting Officer in consultation with the Headquarters or Component CIO and Headquarters or Component Privacy Officer.

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

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

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

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

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

(1) The Contractor shall have in place procedures and the capability to notify any individual whose PII resided in the Contractor IT system at the time of the sensitive information incident not later than 5 business days after being directed to notify individuals, unless otherwise approved by the Contracting Officer. The method and content of any notification by the Contractor shall be coordinated with, and subject to prior written approval by the Contracting

Officer, in consultation with the Headquarters or Component Privacy Officer, utilizing the *DHS Privacy Incident Handling Guidance*. The Contractor shall not proceed with notification unless the Contracting Officer, in consultation with the Headquarters or Component Privacy Officer, has determined in writing that notification is appropriate.

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

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

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

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

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

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

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

(i) A dedicated telephone number to contact customer service within a fixed period;
(ii) Information necessary for registrants/enrollees to access credit reports and credit scores;
(iii) Weekly reports on call center volume, issue escalation (i.e., those calls that cannot be handled by call center staff and must be resolved by call center management or DHS, as appropriate), and other key metrics;

(iv) Escalation of calls that cannot be handled by call center staff to call center management or DHS, as appropriate;
(v) Customized FAQs, approved in writing by the Contracting Officer in coordination with the Headquarters or Component Chief Privacy Officer; and
(vi) Information for registrants to contact customer service representatives and fraud resolution representatives for credit monitoring assistance.

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

(End of clause)

INFORMATION TECHNOLOGY SECURITY AND PRIVACY TRAINING (MAR 2015)

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

(b) *Security Training Requirements*.

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

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

(c) *Privacy Training Requirements.* All Contractor and subcontractor employees that will have access to Personally Identifiable Information (PII) and/or Sensitive PII (SPII) are required to take *Privacy at DHS: Protecting Personal Information* before accessing PII and/or SPII. The training

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

(End of clause)

ACCESSIBILITY REQUIREMENTS (SECTION 508)

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

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

Section 508 Applicable EIT Accessibility Standards

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

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

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

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

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

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

Section 508 Applicable Exceptions

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

Section 508 Compliance Requirements

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

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

ICAM US LABOR MIX								
		Transition Period (2 Months)						
Position	Eagle II Labor Category	FTEs	Hours	Extended Hours	EAGLE II Schedule Rate	Discounted Rate	Extended Price	FTEs
Administrative Task Area (6.1 PWS)								
Project Manager - Level III	Project Manager - Level III							
Technical PM	Project Manager - Level II							
Enterprise Task Area (6.2 PWS)								
Java Programmer /IDM Engineer	Applications Engineer (Senior)/Applications Developer - Level III							
Architect/Engineer	Systems Architect (Solutions Architect - Level III)							
Java Programmer /IDM Engineer	Applications Engineer (Senior)/Applications Developer - Level II							
IDM Tech SME	Subject Matter Expert - Level III							
Access Mgt engineers	Applications Developer - Level SME III							
ID engineering/CI/CD Scripting	Information Engineer/Principal Data Enterprise Architect - Level III							
Agile	Functional Analyst (Scrum Master) Level III							
Agile	Quality Assurance Analyst Level III							
ID engineering/CI/CD Scripting	Information Engineer/Principal System Admin-Level II							
Public Task Area (6.3 PWS)								
ID engineering/CI/CD Scripting	Information Engineer/Principal Data Enterprise Architect - Level III							
Java Programmer /IDM Engineer	Applications Engineer (Senior)/Applications Developer - Level III							
Agile	Functional Analyst (Scrum Master) Level III							
Agile	Quality Assurance Analyst Level III							
Ruby Rails Expert	Application Developers(System Engineers III)							
Legacy Integration Task Area (6.4 PWS)								
ID engineering/CI/CD Scripting	Information Engineer/Principal Data Enterprise Architect - Level III							
ID engineering/CI/CD Scripting	Information Engineer/Principal System Admin-Level II							
Agile	Research Analyst (Tech Writer) Level III							
	Total							
	Total Transition/Base/3 Options							

[redacted] Period (10 Months)						Option 1 (12 Months)					
Hours	Extended Hours	EAGLE II Schedule Rate	Discounted Rate	Extended Price	FTEs	Hours	Extended Hours	EAGLE II Schedule Rate	Discounted Rate	Extended Price	FTEs
[redacted]											

Option 2 (12 Months)					Option 3 (12 Months)					
Hours	Extended Hours	EAGLE II Schedule Rate	Discounted Rate	Extended Price	FTEs	Hours	Extended Hours	EAGLE II Schedule Rate	Discounted Rate	Extended Price
[redacted]										

Section B – Line Item Structure

	Base Period (09/26/17 – 09/25/18)				
Item #	**Description**	**QTY**	**Unit**	**Unit Price**	**Total Amount**
0001	Phase-In, section 6.5 of the PWS (FFP)	[redacted]			
0002	Administrative Task Area, section 6.1 of the PWS (FFP)	[redacted]			
0003	ICAM Enterprise Task Area, section 6.2 of the PWS (FFP)	[redacted]			
0004	ICAM Public Task Area, section 6.3 of the PWS (FFP)	[redacted]			
0005	ICAM Legacy Integration Task Area, section 6.4 of the PWS (FFP)	[redacted]			
Total Base					
	Option Period 1 (09/26/18 – 09/25/19)				
Item #	**Description**	**QTY**	**Unit**	**Unit Price**	**Total Amount**
1002	Administrative Task Area, section 6.1 of the PWS (FFP)	[redacted]			
1003	ICAM Enterprise Task Area, section 6.2 of the PWS (FFP)	[redacted]			
1004	ICAM Public Task Area, section 6.3 of the PWS (FFP)	[redacted]			
1005	ICAM Legacy Integration Task Area, section 6.4 of the PWS (FFP)	[redacted]			
Total Option 1					
	Option Period 2 (09/26/19 – 09/25/20)				
Item #	**Description**	**QTY**	**Unit**	**Unit Price**	**Total Amount**
2002	Administrative Task Area, section 6.1 of the PWS (FFP)	[redacted]			
2003	ICAM Enterprise Task Area, section 6.2 of the PWS (FFP)	[redacted]			
2004	ICAM Public Task Area, section 6.3 of the PWS (FFP)	[redacted]			
2005	ICAM Legacy Integration Task Area, section 6.4 of the PWS (FFP)	[redacted]			
Total Option 2					
	Option Period 3 (09/26/20 – 09/25/21)				
Item #	**Description**	**QTY**	**Unit**	**Unit Price**	**Total Amount**
3002	Administrative Task Area, section 6.1 of the PWS (FFP)	[redacted]			
3003	ICAM Enterprise Task Area, section 6.2 of the PWS (FFP)	[redacted]			
3004	ICAM Public Task Area, section 6.3 of the PWS (FFP)	[redacted]			
3005	ICAM Legacy Integration Task Area, section 6.4 of the PWS (FFP)	[redacted]			
Total Option 3					
	Transition, Base and 3 Options				
Total					