ORDER FOR SUPPLIES OR SERVICES

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

PAGE OF PAGES
1 44

1. DATE OF ORDER
MAR 2 3 2018

2. CONTRACT NO. *(If any)*
HSHQDC-13-D-E2105

3. ORDER NO.
70SBUR18F00000063

4. REQUISITION/REFERENCE NO.
VER180033

5. ISSUING OFFICE *(Address correspondence to)*
USCIS Contracting Office
Department of Homeland Security
70 Kimball Avenue
South Burlington VT 05403

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

f. SHIP VIA

7. TO:

a. NAME OF CONTRACTOR
ATTAIN LLC

b. COMPANY NAME

c. STREET ADDRESS
1600 TYSONS BLVD
STE 1400

d. CITY
MCLEAN

e. STATE
VA

f. ZIP CODE
221024893

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
Verification Division

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
Destination

13. PLACE OF

a. INSPECTION
Destination

b. ACCEPTANCE
Destination

14. GOVERNMENT B/L NO.

15. DELIVER TO F.O.B. POINT ON OR BEFORE *(Date)*
Multiple

16. DISCOUNT TERMS
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: 831112466+0000 Task order for Verification DevOpsSec (VDOS) EAGLE II FC 1 Unrestricted Period of Performance: Base: 04/14/2018-04/13/2019 Continued ...					

SEE BILLING INSTRUCTIONS ON REVERSE

18. SHIPPING POINT

19. GROSS SHIPPING WEIGHT

20. INVOICE NO.

21. MAIL INVOICE TO:

a. NAME
See Invoicing Instructions

b. STREET ADDRESS (or P.O. Box)

c. CITY

d. STATE

e. ZIP CODE

17(h) TOTAL (Cont. pages) ▶ $4,714,003.20

17(i) GRAND TOTAL ▶ $4,714,003.20

22. UNITED STATES OF AMERICA BY *(Signature)* ▶ Charles E

MAR 2 3 2018

23. NAME *(Typed)*
CHARLES E. JULIAN
TITLE: CONTRACTING/ORDERING OFFICER

AUTHORIZED FOR LOCAL REPRODUCTION
PREVIOUS EDITION NOT USABLE

ORDER FOR SUPPLIES OR SERVICES
SCHEDULE - CONTINUATION

PAGE NO
2

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

DATE OF ORDER	CONTRACT NO. HSHQDC-13-D-E2105	ORDER NO. 70SBUR18F00000063

ITEM NO. (a)	SUPPLIES/SERVICES (b)	QUANTITY ORDERED (c)	UNIT (d)	UNIT PRICE (e)	AMOUNT (f)	QUANTITY ACCEPTED (g)
	Option 1: 04/14/2019/04/13/2020 AAP Number: None DO/DPAS Rating: NONE Accounting Info: VISVDOS 000 OS 70-01-00-000 07-20-0200-00-00-00-00 GE-25-76-00 000000					
0001	Transition in (3 months)(Firm Fixed Price) Per Section 5 of the Statement of Work (Not Separately Priced)	1	LO		0.00	
0001 AA	Transition in (Firm Fixed Price) Delivery: 60 Days After Receipt of Order	1	MO	[redacted]	[redacted]	
0001 AB	Transition in (Firm Fixed Price) Delivery: 90 Days After Award	1	MO	[redacted]	[redacted]	
0001 AC	Transition in (Firm Fixed Price) Delivery: 120 Days After Award	1	MO	[redacted]	[redacted]	
0002	Key Personnel and Matrixed DevOpsSec Team (Firm Fixed Price)	9	MO	[redacted]	[redacted]	
0003	DevSecOps Team #1(Firm Fixed Price)	9	MO	[redacted]	[redacted]	
0004	DevSecOps Team #2(Firm Fixed Price)	9	MO	[redacted]	[redacted]	
1001	Key Personnel and Matrixed DevSecOps Team (Firm Fixed Price) Amount: [redacted](Option Line Item) Anticipated Exercise Date:04/14/2019	9	MO	[redacted]	[redacted]	
1002	DevSecOps Team #1(Firm Fixed Price) Amount: [redacted](Option Line Item) Anticipated Exercise Date:04/14/2019 Continued ...	9	MO	[redacted]	[redacted]	

TOTAL CARRIED FORWARD TO 1ST PAGE (ITEM 17(H)) ▷ $4,714,003.20

ORDER FOR SUPPLIES OR SERVICES
SCHEDULE - CONTINUATION

PAGE NO
3

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

DATE OF ORDER	CONTRACT NO.	ORDER NO.
	HSHQDC-13-D-E2105	70SBUR18F00000063

ITEM NO. (a)	SUPPLIES/SERVICES (b)	QUANTITY ORDERED (c)	UNIT (d)	UNIT PRICE (e)	AMOUNT (f)	QUANTITY ACCEPTED (g)
1003	DevSecOps Team #2 (Firm Fixed Price) Amount: [redacted](Option Line Item) Anticipated Exercise Date:04/14/2019	9	MO	[redacted]	[redacted]	
1004	Transition out (3 months)(Firm Fixed Price) Per Section 5 of the Statement of Work Amount: $0.00(Option Line Item) Anticipated Exercise Date:01/14/2020 (Not Separately Priced)	1	LO	[redacted]	[redacted]	
1004 AA	Transition out(Firm Fixed Price) Amount: [redacted](Option Line Item) Anticipated Exercise Date:01/14/2020	1	MO	[redacted]	[redacted]	
1004 AB	Transition out(Firm Fixed Price) Amount: [redacted](Option Line Item) Anticipated Exercise Date:02/14/2020	1	MO	[redacted]	[redacted]	
1004 AC	Transition out(Firm Fixed Price) Amount: [redacted](Option Line Item) Anticipated Exercise Date:03/14/2020	1	MO	[redacted]	[redacted]	
	Part II - Contract Clauses: 1. Contract Clauses 2. Accessibility Requirements (Section 508) 3. Security Clause 5 w/IT 4. Safeguarding of Sensitive Information 5. Information Technology Security and Privacy Training 6. DHS Enterprise Architecture Compliance 7. Capitalized Property, Plant & Equipment (PP&E) Assets Internal Use Software (IUS)					
	Part III - Documents, exhibits, or attachments: 1. Statement of Work 2. DevOpsSec Team(s) Eagle II Labor Categories and Levels Continued ...					

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

ORDER FOR SUPPLIES OR SERVICES
SCHEDULE - CONTINUATION

PAGE NO
4

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

DATE OF ORDER	CONTRACT NO.	ORDER NO.
	HSHQDC-13-D-E2105	70SBUR18F00000063

ITEM NO. (a)	SUPPLIES/SERVICES (b)	QUANTITY ORDERED (c)	UNIT (d)	UNIT PRICE (e)	AMOUNT (f)	QUANTITY ACCEPTED (g)
	The total amount of award: [redacted]. The obligation for this award is shown in box 17(i).					
	TOTAL CARRIED FORWARD TO 1ST PAGE (ITEM 17(H)) ▷				$0.00	

Part II-Contract Clauses

1. **CONTRACT CLAUSES:**
   This order will be subject to the EAGLE II IDIQ FC1 Unrestricted Contract Terms and Conditions

Federal Acquisition Regulation (FAR) clauses incorporated by reference

52.209-10	Prohibition on Contracting with Inverted Domestic Corporations	(Nov 2015)
52.224-3	Privacy Training	(Jan 2017)
	Alternate I	(Jan 2017)
52.232-39	Unenforceability of Unauthorized Obligations	(Jun 2013)
52.232-40	Providing Accelerated Payments to Small Business Subcontractors	(Dec 2013)
52.237-3	Continuity of Services	(Jan 1991)

Federal Acquisition Regulation (FAR) clauses incorporated in full text

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

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

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

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

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

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

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

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

(e) In accordance with section 743 of Division E, Title VII, of the Consolidated and Further Continuing Appropriations Act, 2015, (Pub. L. 113-235), and its successor provisions in subsequent appropriations acts (and as extended in continuing resolutions) use of funds appropriated (or otherwise made available) is prohibited, if the Government determines that the Contractor is not in compliance with the provisions of this clause.

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

(End of clause)

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

(a) The Government may extend the term of this contract by written notice to the Contractor within **15** days; 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 **24 months**.

52.252-4 Alterations in Contract (Apr 1984)

Portions of this contract are altered as follows:

> Use of the word "contract" is understood to mean "task order" whenever such application is appropriate.
>
> 52.244-2 has been deleted

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

3052.215-70 Key Personnel or Facilities (Dec 2003)

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

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

The Key Personnel under this Contract are:

Program Manger

Solutions Architect/Technical Lead

(End of clause)

3052.204-71 Contractor Employee Access Alt I (SEP 2012)

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

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

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

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

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

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

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

(d) The Contracting Officer may require the Contractor to prohibit individuals from working on the contract if the Government deems their initial or continued employment contrary to the public interest for any reason, including, but not limited to, carelessness, insubordination, incompetence, or security concerns.

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

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

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

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

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

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

(k) Non-U.S. citizens shall not be authorized to access or assist in the development, operation, management or maintenance of Department IT systems under the contract, unless a waiver has been granted by the Head of the Component or designee, with the concurrence of both the Department's Chief Security Officer (CSO) and the Chief Information Officer (CIO) or their designees. Within DHS Headquarters, the waiver may be granted only with the approval of both the CSO and the CIO or their designees. In order for a waiver to be granted:

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

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

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

(End of clause)

Local Clauses

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

EXPECTATION OF CONTRACTOR PERSONNEL

The Government expects competent, productive, qualified IT professionals to be assigned to the Agile teams.

PERFORMANCE REPORTING

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

FINAL PAYMENT

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

GOVERNMENT-FURNISHED PROPERTY

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

Equipment	QTY	unit	unit acquisition cost
Laptop computer	20	EA	$ 4,500
Mobile Device	2	EA	$ 500

(b) The Government will issue laptop computers to no more than twenty (20) 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.

NOTICE TO PROCEED (NTP)

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

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

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

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

(e) The Government intends for the transition CLIN to begin once the contractor has successfully obtained a suitability clearance. The contracting officer will issue a phase-in notice to proceed (PNTP) once the contractor has EOD all Key Personnel including the Project Manager and the Solutions Architect/ Tech Lead positions under the Key Personnel section 4 of the SOW. This notice will be given at least one day before transition is to begin.

(f) The transition period shall last for 90 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 notice to proceed (NTP) once an entire Agile team has EOD. The notice will be given at least one day before full performance is to begin.

A NTP will not be issued by the Contracting Officer until such time as satisfactory suitability determinations have been received and successfully processed by the USCIS Office of Security & Integrity for an entire Agile team. The Notice to Proceed shall specifically identify the Contract Line Items (CLIN) (or sub-Contract Line Items – sub-CLIN) affected. In this manner the government can be clear as to which line items or sub-line items are in compliance with the SOW in terms of staffing and thus able to begin full performance.

Regarding staffing, the contractor shall request through the COR to the CO to receive a Notice to Proceed once all contractor personnel for a particular CLIN or sub-CLIN have a valid EOD. If all required EOD dates are received prior to the 15th of the month, the NTP shall include the entire month in which the request was made. If EOD dates are received and an NTP requested after the 15th of the month, the NTP start cite a start date aligning with the next full month.

For those CLINs or sub-CLINs not included in the initial full performance NTP, the duration of their performance period shall be such that it ends at the same time as those started with the initial full performance NTP. Individual CLINs or sub-CLINs shall not have staggered end dates. An NTP issued after the initial full performance NTP shall capture the revised performance period per each CLIN or sub-CLIN associated with the Notice.

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.

2. ACCESIBILITY 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 ET 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.

3. SECURITY CLAUSE 5 w/ IT

GENERAL

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

SUITABILITY DETERMINATION

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

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

BACKGROUND INVESTIGATIONS

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

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

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

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

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

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

4. Position Designation Determination for Contract Personnel Form

5. Foreign National Relatives or Associates Statement

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

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

EMPLOYMENT ELIGIBILITY

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

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

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

CONTINUED ELIGIBILITY

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

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

In support of the overall USCIS mission, Contractor employees are required to complete one-time or annual DHS/USCIS mandatory trainings. The Contractor shall certify annually, but no later than December 31st each year, or prior to any accelerated deadlines designated by USCIS, that required trainings have been completed. The certification of the completion of the trainings by all contractors shall be provided to both the COR and Contracting Officer.

- **USCIS Security Awareness Training** (required within 30 days of entry on duty for new contractors, and annually thereafter)
- **USCIS Integrity Training** (Annually)
- **DHS Continuity of Operations Awareness Training** (one-time training for contractors identified as providing an essential service)
- **Unauthorized Disclosure Training** (one time training for contractors who require access to USCIS information regardless if performance occurs within USCIS facilities or at a company owned and operated facility)
- **USCIS Fire Prevention and Safety Training** (one-time training for contractors working within USCIS facilities; contractor companies may substitute their own training)

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

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

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

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

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

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

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

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

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

SECURITY MANAGEMENT

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

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

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

SECURITY PROGRAM BACKGROUND

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

- Public Law 107-296, Homeland Security Act of 2002.
- Federal Information Security Management Act (FISMA) of 2002, November 25, 2002.
- Public Law 104-106, Clinger-Cohen Act of 1996 [formerly, Information Technology Management Reform Act (ITMRA)], February 10, 1996.
- Privacy Act of 1974, As Amended. 5 United States Code (U.S.C.) 552a, Public Law 93-579, Washington, D.C., July 14, 1987.
- Executive Order 12829, *National Industrial Security Program*, January 6, 1993.
- Executive Order 12958, *Classified National Security Information*, as amended.
- Executive Order 12968, *Access to Classified Information,* August 2, 1995.
- Executive Order 13231, *Critical Infrastructure Protection in the Information Age*, October 16, 2001
- National Industrial Security Program Operating Manual (NISPOM), February 2001.
- DHS *Sensitive Systems Policy Publication 4300A* v2.1, July 26, 2004
- DHS *National Security Systems Policy Publication 4300B* v2.1, July 26, 2004
- Homeland Security Presidential Directive 7, *Critical Infrastructure Identification, Prioritization, and Protection*, December 17, 2003.
- Office of Management and Budget (OMB) Circular A-130, *Management of Federal*
- *Information Resources.*
- National Security Directive (NSD) 42, *National Policy for the Security of National Security Telecommunications and Information Systems* (U), July 5, 1990, CONFIDENTIAL.
- 5 Code of Federal Regulations (CFR) §2635, Office of Government Ethics, *Standards of Ethical Conduct for Employees of the Executive Branch.*
- DHS SCG OS-002 (IT), National Security IT Systems Certification & Accreditation, March 2004.
- Department of State 12 Foreign Affairs Manual (FAM) 600, *Information Security*
- *Technology*, June 22, 2000.
- Department of State 12 FAM 500, *Information Security*, October 1, 1999.
- Executive Order 12472, *Assignment of National Security and Emergency Preparedness Telecommunications Functions*, dated April 3, 1984.
- Presidential Decision Directive 67, *Enduring Constitutional Government and Continuity of Government Operations*, dated October 21, 1998.
- FEMA Federal Preparedness Circular 65, *Federal Executive Branch Continuity of Operations (COOP)*, dated July 26, 1999.
- FEMA Federal Preparedness Circular 66, *Test, Training and Exercise (TT&E) for Continuity of Operations (COOP)*, dated April 30, 2001.
- FEMA Federal Preparedness Circular 67, *Acquisition of Alternate Facilities for Continuity of Operations*, dated April 30, 2001.

- Title 36 Code of Federal Regulations 1236, Management of Vital Records, revised as of July 1, 2000.
- National Institute of Standards and Technology (NIST) Special Publications for computer security and FISMA compliance.

GENERAL

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

IT SYSTEMS SECURITY

In accordance with DHS Management Directive 4300.1 "Information Technology Systems Security", USCIS Contractors shall ensure that all employees with access to USCIS IT Systems are in compliance with the requirement of this Management Directive. Specifically, all contractor employees with access to USCIS IT Systems meet the requirement for successfully completing the annual "Computer Security Awareness Training (CSAT)." All contractor employees are required to complete the training within 60-days from the date of entry on duty (EOD) and are required to complete the training yearly thereafter.
CSAT can be accessed at the following: http://otcd.uscis.dhs.gov/EDvantage.Default.asp or via remote access from a CD which can be obtained by contacting uscisitsecurity@dhs.gov.

IT SECURITY IN THE SYSTEMS DEVELOPMENT LIFE CYCLE (SDLC)

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

- *Sensitive System Security Plan (SSSP)*: This is the primary reference that describes system sensitivity, criticality, security controls, policies, and procedures. The SSSP shall be based upon the completion of the DHS FIPS 199 workbook to categorize the system of application and completion of the RMS Questionnaire. The SSSP shall be completed as part of the System or Release Definition Process in the SDLC and shall not be waived or tailored.
- *Privacy Impact Assessment (PIA) and System of Records Notification (SORN).* For each new development activity, each incremental system update, or system recertification, a PIA and SORN shall be evaluated. If the system (or modification)

triggers a PIA the contractor shall support the development of PIA and SORN as required. The Privacy Act of 1974 requires the PIA and shall be part of the SDLC process performed at either System or Release Definition.

- *Contingency Plan (CP)*: This plan describes the steps to be taken to ensure that an automated system or facility can be recovered from service disruptions in the event of emergencies and/or disasters. The Contractor shall support annual contingency plan testing and shall provide a Contingency Plan Test Results Report.
- *Security Test and Evaluation (ST&E)*: This document evaluates each security control and countermeasure to verify operation in the manner intended. Test parameters are established based on results of the RA. An ST&E shall be conducted for each Major Application and each General Support System as part of the certification process. The Contractor shall support this process.
- *Risk Assessment (RA):* This document identifies threats and vulnerabilities, assesses the impacts of the threats, evaluates in-place countermeasures, and identifies additional countermeasures necessary to ensure an acceptable level of security. The RA shall be completed after completing the NIST 800-53 evaluation, Contingency Plan Testing, and the ST&E. Identified weakness shall be documented in a Plan of Action and Milestone (POA&M) in the USCIS Trusted Agent FISMA (TAF) tool. Each POA&M entry shall identify the cost of mitigating the weakness and the schedule for mitigating the weakness, as well as a POC for the mitigation efforts.
- *Certification and Accreditation (C&A):* This program establishes the extent to which a particular design and implementation of an automated system and the facilities housing that system meet a specified set of security requirements, based on the RA of security features and other technical requirements (certification), and the management authorization and approval of a system to process sensitive but unclassified information (accreditation). As appropriate the Contractor shall be granted access to the USCIS TAF and Risk Management System (RMS) tools to support C&A and its annual assessment requirements. Annual assessment activities shall include completion of the NIST 800-26 Self-Assessment in TAF, annual review of user accounts, and annual review of the FIPS categorization. C&A status shall be reviewed for each incremental system update and a new full C&A process completed when a major system revision is anticipated.

SECURITY ASSURANCES

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

- *User Identification and Authentication (I&A)* – I&A is the process of telling a system the identity of a subject (for example, a user) (*I*) and providing that the subject is who it claims to be (*A*). Systems shall be designed so that the identity of each user shall be established prior to authorizing system access, each system user shall have his/her own user ID and password, and each user is authenticated before access is permitted. All system and database administrative users shall have strong authentication, with passwords that shall conform to established DHS standards. All USCIS Identification and Authentication shall be done using the Password Issuance Control System (PICS) or its successor. Under no circumstances will Identification and Authentication be performed by other than the USCIS standard system in use at the time of a systems development.

- *Discretionary Access Control (DAC)* – DAC is a DHS access policy that restricts access to system objects (for example, files, directories, devices) based on the identity of the users and/or groups to which they belong. All system files shall be protected by a secondary access control measure.
- *Object Reuse* – Object Reuse is the reassignment to a subject (for example, user) of a medium that previously contained an object (for example, file). Systems that use memory to temporarily store user I&A information and any other SBU information shall be cleared before reallocation.
- *Audit* – DHS systems shall provide facilities for transaction auditing, which is the examination of a set of chronological records that provide evidence of system and user activity. Evidence of active review of audit logs shall be provided to the USCIS IT Security Office on a monthly basis, identifying all security findings including failed log in attempts, attempts to access restricted information, and password change activity.
- *Banner Pages* – DHS systems shall provide appropriate security banners at start up identifying the system or application as being a Government asset and subject to government laws and regulations. This requirement does not apply to public facing internet pages, but shall apply to intranet applications.

DATA SECURITY

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

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

- *Data Labeling.* – The contractor shall ensure that documents and media are labeled consistent with the DHS *Sensitive Systems Handbook.*

4. HSAR CLASS DEVIATION 15-01: SAFEGUARDING OF SENSITIVE INFORMATION (MAR 2015)

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

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

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

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

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

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

(2) Sensitive Security Information (SSI), as defined in Title 49, Code of Federal Regulations,

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

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

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

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

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

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

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

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

(1) DHS Management Directive 11042.1 Safeguarding Sensitive But Unclassified (for Official Use Only) Information
(2) DHS Sensitive Systems Policy Directive 4300A
(3) DHS 4300A Sensitive Systems Handbook and Attachments
(4) DHS Security Authorization Process Guide

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

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

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

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

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

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

(e) *Authority to Operate*. The Contractor shall not input, store, process, output, and/or transmit sensitive information within a Contractor IT system without an Authority to Operate (ATO) signed by the Headquarters or Component CIO, or designee, in consultation with the Headquarters or Component Privacy Officer. Unless otherwise specified in the ATO letter, the

ATO is valid for three (3) years. The Contractor shall adhere to current Government policies, procedures, and guidance for the Security Authorization (SA) process as defined below.

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

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

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

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

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

5. 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 email notification shall state the required training has been completed for all Contractor and subcontractor employees.

(End of clause)

6. DHS ENTERPRISE ARCHITECTURE COMPLIANCE

"All solutions and services shall meet DHS Enterprise Architecture policies, standards, and procedures. Specifically, the Government intends to:

a) All developed solutions and requirements shall be compliant with the Homeland Security Enterprise Architecture (HLS EA).

b) All IT hardware and software shall be compliant with the HLS EA Technical Reference Model (TRM) Standards and Products Profile.

c) Description information for all data assets, information exchanges and data standards, whether adopted or developed, shall be submitted to the Enterprise Data Management Office (EDMO) for review, approval and insertion into the DHS Data Reference Model and Enterprise Architecture Information Repository.

d) Development of data assets, information exchanges and data standards will comply with the DHS Data Management Policy MD 103-01 and all data-related artifacts will be developed and validated according to DHS data management architectural guidelines.

e) Applicability of Internet Protocol Version 6 (IPv6) to DHS-related components (networks, infrastructure, and applications) specific to individual acquisitions shall be in accordance with the DHS Enterprise Architecture (per OMB Memorandum M-05-22, August 2, 2005) regardless of whether the acquisition is for modification, upgrade, or replacement. All EA-related component acquisitions shall be IPv6 compliant as defined in the U.S. Government Version 6 (USGv6) Profile (National Institute of Standards and Technology (NIST) Special Publication 500-267) and the corresponding declarations of conformance defined in the USGv6 Test Program. "

7. CAPITALIZED PROPERTY, PLANT & EQUIPMENT (PP&E) ASSETS INTERNAL USE SOFTWARE (IUS)

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.

Requirement

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

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

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

The contractor shall, after OIT's determination on whether or not the release meets the capitalization criteria, support OIT's reporting of costs incurred for the project or release, as required. The contractor shall provide the nature and cost of work completed within the relevant period. Costs considered part of IUS activities include systems administration, systems engineering, and program management. The contractor shall provide the total cost, itemized by release and include the total sum of all applicable IUS activities. At the contractor's discretion, this information may be submitted, either as an attachment or as an itemized line item within the monthly invoices, as outlined in Table 3: Resource Expenditure Format and Figure 1: Resource Expenditure Format. 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.

Part III - Documents, exhibits, or attachments

1. Statement of Work

1. OVERVIEW

Verification DevOpsSec (VDOS) will be a lightweight, rapid, and flexible procurement for Development Operations and Security (DevOpSec) services to support United States Citizenship and Immigration Services Information Technology (USCIS) (IT) system delivery. USCIS's goal is to move rapidly to award and onboard contractor staff, while continuously improving its internal acquisition processes to make them as lean as possible.

The VDOS contractor will provide two DevOpSec Teams and (1) Key Personnel and Matrixed Team. The VDOS teams will perform DevOpSec services for components of the Verification system, which is hosted in the Amazon Web Services (AWS) cloud, and/or the Department of Homeland Security (DHS) Infrastructure as a Service (IaaS) cloud or other specified clouds. The team will include "full stack" expertise and will have the full set of responsibilities for development, operations, security, and testing of a set of capabilities in development, test, stage and production environments. The VDOS contractor will use a Continuous Integration / Continuous Delivery (CI/CD) approach and pipeline and is expected to adopt cutting edge best practices for IT delivery.

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

The Team structure will adhere to the following requirements:

- Key Personnel and Matrixed Team – Consists of five (5) people that includes a Program Manager, a Scrum Master/Agile Lead, Database Specialist (DBA), Systems Operations Specialist, And Solutions Architect/Tech Lead.
- Team #1– Consists of six (6) people that includes a mix of developers/testers, full stack engineers, and Microsoft Dynamics subject matter experts.
- Team #2– Consists of nine (9) people that includes a mix of developers/testers, full stack engineers, UX/UI designers, and business analysts.

The base period will consist of a three (3) month transition in Firm Fixed Price (FFP) CLIN and a nine (9) month FFP, with the subsequent twelve (12) month option period set up as a nine (9) month FFP CLIN and a three (3) month transition out CLIN. The Partial Notice to Proceed (NTP) will not be granted until all key personnel have received their EOD and there have been a minimum of 70% of contractors who have received their EOD to perform the work as determined by the Government Program Manager (GPM) and CO. A Full NTP will not be issued by the Contracting Officer until such time as satisfactory suitability determinations have been received and successfully processed by the USCIS Office of Security & Integrity for an entire Agile team.

2. SCOPE

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

Critical elements of the VDOS team will be:

- High productivity
- High quality work
- High level of initiative and ownership
- Collaboration and cooperation with other USCIS teams and participants
- Technical skills and expertise as necessary (see below)
- Estimation and planning skills
- Innovation and creativity in problem solving

As DHS requires Section 508- compliant user interfaces, the contractor shall accredit a member of the team as a Section 508 DHS Trusted Tester within the 6 months of EOD. This individual must be properly vetted and certified at the start of the contract. The provider of VDOS services shall adopt evolving USCIS design and coding standards in the course of their application development. The contractor shall provide technical methods, techniques, and concepts that are innovative, practical, cost-effective, and conducive to agile application development. The contractor shall develop IT capabilities based on requirements that are evolving and emerge as the business climate shifts.

VDOS developers will be required to develop high quality code and are responsible for any technical debt that is incurred as a result of their development activities. VDOS developers shall intelligently balance core productivity with technical debt, and are not expected to use high productivity standards as an excuse for cutting corners. Technical debt should be addressed as it occurs and should not become so overwhelming that it must be addressed using an entire or several entire sprints.

Services in support of VDOS shall be provided by experts with demonstrated experience in using USCIS specified tools and technologies as described in section *2.1 Technical Landscape*. DevOps involves some degree of analysis, requirements collection, design, development, test, platform engineering, and production operations in addition to the support functions of configuration management, planning, and project management. In addition, DevOps should be considered to be "infrastructure as code" with the mindset and practice of automating through code everything possible. The specific tasks applicable under this task order are detailed in section *3 TASKS.* Delivery and operation are expected to follow agile and DevOps industry best practices.

2.1 Technical Landscape

The contractor shall use USCIS enclaves in the AWS public cloud, DHS private cloud, and/or other cloud environment specified by the Government, for development, testing, and production. Testing shall primarily be automated, reflecting the best-practice "testing pyramid" with an emphasis on excellent code coverage through unit tests. Unit test should cover a minimum of 80% of the code and the contractor shall provide at least monthly reporting on code coverage and technical debt to the government. The build pipeline will also include USCIS standard tools for code standards, test coverage, security testing, and section 508 compliance.

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

The VDOS contract will use the USCIS standard platform and tools. This platform will evolve over time to continue to fit the needs of USCIS and the VDOS contract will need to embrace and support an ever evolving tool stack. The current platform is described in the chart below:

Name	Function
AWS Cloud	Public cloud platform. USCIS currently uses EC2, S3, ECR, RDS, CloudFormation, Lambda, and a number of other AWS services
Amazon Linux / RHEL / CentOS	RedHat-based Operating Systems
Apache ActiveMQ	Messaging Provider
Apache Commons Libs	Java software library
Apache Jmeter	Performance testing
Apache Tomcat	Application server
Artifactory	Repository manager
ASP.NET	Programming Language
BouncyCastle (FIPS)	Crytography API
Chaos Monkey	Application Resiliency Tool
Chef	Deployment scripting
Cucumber/Jasmine/Selenium	Integration Testing
Customer Care Desktop	UII framework
DeQue FireEyes	508 Development Test tool
Docker	Containerization
Fortify	Security test tool
Git / Enterprise GitHub	Distributed version control
Java	Programming Language
Java Mail	Email message generation

JAXB	Java Representation of XML
Jenkins	Continuous integration server
Jira	Agile lifecycle management tool
JUnit	Java Unit testing library
Maven	Java artifacts and dependency managements framework
Microsoft Dynamics	Customer Relationship Management tool
Microsoft SQL Server	Database server
Mule ESB	Enterprise Service Bus/Integration Platform
New Relic	Application and Infrastructure Monitoring
Nexus	Repository manager
Oracle	Database/Reporting
POI	Excel file generation
rspec	Unit Testing
Ruby	Programming Language
Rails	Web Application Framework
SiteMesh	Java web application framework
Snap	Continuous integration and delivery platform
SoapUI	WebService Testing tool
Spring Framework	Application Framework
SSRS	SQL Server Reporting Services
Terraformer	Cloud resource creating and management tool
Unified Service Desk	UII framework
Windows Server	Operating System
Microsoft.net	Application Code
IIS Webser	Webserver

Table 1: Current Tool Suite and Platforms

3 TASKS

The tasks identified in the following sections describe the work that will comprise the VDOS task order. The VDOS contractor shall propose 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 2.*1 Technical Landscape.*

3.1 Provide DevOpSec Teams

The contractor shall provide one team, the key personnel and a matrixed support team, that consists of five (5) individuals, which includes a Program Manager, a Solutions Architect/Tech Lead, a Scrum Master/Agile Lead, Database Specialist (DBA), and a Systems Operations Specialist. A second team that consists of six (6 people) that includes a mix of developers/testers, full stack .NET and Java engineers, and hands-on Microsoft Dynamics subject matter experts. The third team that consists of nine (9) people, which includes a mix of developers/testers, full stack .NET and Java engineers, UX/UI designers, and business analysts.

Note: The contractor should use a test driven development (TDD) approach. The contractor's work shall conform to the architecture and design provided by USCIS and the agile processes set up by USCIS but managed by the teams specifically. The teams must have all of the skills necessary to perform the tasks indicated in this section. It is important that the team as a whole have the skills necessary for development, operations, security, and test– but that does **not** mean that specific team members must be designated as testers, coders, etc. Most of the team members should have more than one skill, for example. It is up to the contractor to structure the team so that it can provide all of the necessary functions at a high level of productivity and quality. The team construct should follow the guidance in the overview section. The team should be experienced with the latest technologies and languages and the AWS cloud.

3.2 Development

The contractor shall be responsible for the teams that perform the full suite of DevOps tasks using agile methodologies, including but not limited to participating in creating user stories for both business functionality and technical requirements and defining acceptance criteria; estimating the size of stories; designing solutions; developing code and automated tests; creating deployment scripts; managing code in production; managing any Database solutions. The contractor shall test its product and ensure its quality; and shall deploy its code.

3.3 Documentation

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.

The contractor shall document system design and procedures in the wiki that USCIS uses for a System Design Document (SDD) concurrent with development activities. In general, USCIS prefers relatively lightweight (minimal language with sufficient details) but effective and usable documentation.

3.4 Design

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

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

3.5 Test and Integration

The contractor shall be responsible for creating test cases and automated test scripts to support test automation activities. Automated tests are considered an important deliverable for the VDOS contractor.

The contractor's code shall meet the functional and non-functional requirements, and the automated and manual tests performed shall verify that it does so. Code and tests will be reviewed by USCIS OIT Independent Validation & Verification (IV&V) to ensure that the testing is appropriate, adequate, and effective, and that it mitigates key risks.

The contractor shall use continuous integration and continuous delivery techniques. Code shall be deployed to production at least weekly, with preference of daily releases to production in small change sets. The system shall be deployable at any time.

- Contractor shall deploy features such that the government can decide when the features will be activated.

- Contractor shall assist with crafting validation steps (both positive and negative testing) for user acceptance testing on an as needed basis.

The contractor shall perform security scans and automated testing with each build to support ongoing authorization and continuously improved security posture.

The contractor shall perform automated load and performance testing with every deployment. In addition, the contractor shall provide a mechanism or manage the mechanism to provide regular reporting on application performance.

The contractor shall perform automated integration testing with all external connections and applications.

3.6 Operations

The contractor shall be responsible for the operation in production of the capabilities they develop.

The contractor shall build in monitoring triggers to effectively reveal production issues in a timely fashion.

The contractor shall provide root cause analysis on all outages with actionable recommendations on how to prevent issues going forward.

The contractor shall ensure that the system is monitored effectively to reveal any production issues when they happen and to monitor the performance of the application.

The contractor shall ensure that the systems are monitored effectively to reveal user analytics and interactions and provide the capability to automatically report on such activities.

The contractor shall ensure that there is an automated way to monitor for network-related production issues providing the capability to rule out application issues.

The primary responsibility for monitoring production systems is held by the USCIS Network Operations Center (NOC). The contractor shall ensure that appropriate monitoring is in place and work with the USCIS NOC on monitoring alerts and escalation processes.

While USCIS expects the quality of the development to not require it, in the event of a critical or high severity production issue, the contractor shall be available to restore system availability and functioning 24x7.

3.7 Administrative Activities

The contractor shall collaborate with stakeholders, support contractors, and third party vendors throughout system integration, performance, security, Section 508, system acceptance, user acceptance, usability, and test and evaluation reporting.

The contractor shall manage all contractor resources and supervise all contractor staff in the performance of work on this task order. The contractor shall manage and coordinate its team(s) on a day-to-day basis and ensure plans are communicated to team members.

Likewise, the contractor must ensure that the health and progress against those plans are adequately reported.

The contractor shall organize, direct and coordinate planning and execution of all task order activities.

Vehicles for transparency, such as the agency Agile Application Lifecycle Management (ALM) tool, shall be maintained with data so that reports and charts can be generated as needed, and so that user stories, defects, 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.

4 KEY PERSONNEL

The contractor shall identify key personnel and provide statements of qualifications for these individuals as a part of the solicitation process. Key personnel shall be current or contingent full time employees of the contractor. The contractor shall identify key personnel who shall be the Program Manager and a Solution architect/engineer for the task order. These individuals must have extensive expertise in the agile and DevOps approaches, and experience using many of the tools included in the Development/Test Tool Suite identified previously. Since this is a team-oriented contract, all of the key personnel may have other duties (for example, the Solutions Architect may also act as a developer and the Program Manager might also act as a business analyst, tester, or Scrum Master), as long as they are able to perform their duties as within the realm specified as key personnel.

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

Key Personnel Minimum Qualifications:

- **Program Manager shall have the following:**
  - A minimum of ten (10) years of IT (Information Technology) Project Management experience, focusing on development projects;
  - Two (2) years specialized experience in managing IT DevOps projects;
  - Bachelor's degree in Computer Science, Information Technology Management or Engineering, or other comparable degree or five (5) years of experience in this arena; and
  - At least five (5) years of experience managing scrum team(s).
- **Solutions Architect/Tech Lead shall have the following:**
  - A minimum of ten (10) years experience in the IT field focusing on development projects;
  - Possess a minimum of 3 years of architecture & design experience (in deploying enterprise applications on AWS in a DevOps capacity;
  - Possess at least 4 years of experience architecting in large scale, high performance enterprise application DevOps architecture on complex heterogeneous environments; and
  - At a minimum, possess a Bachelor's degree in Computer Science, Information Technology Management or Engineering, or other comparable degree or experience.

5 TRANSITION SUPPORT

Upon notice to proceed is granted, the Contractor transition in will begin with the first sprint in accordance with Agile principles, knowledge acquisition is expected to occur within iterations or in the process of performing tasks in the Scrum or Kanban process.

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

Because the contractor will have automated the development, test, and deployment pipeline, and because the contractor will have documented important design decisions and processes in the SDD, the government will expect the transition to go smoothly and efficiently. If it does not, this will indicate to the government, problems in how the tasks of the contract were executed and will be reflected in the contractor's CPARS rating.

The contractor shall be responsible for the implementation of the transition and application cutover activities. The transition shall cause no disruption in development services. To ensure the necessary continuity of services and to maintain the current level of support, USCIS may retain services of the incumbent Contractor for some, or all of, the transition period, as may be required.

The contractor shall be responsible for the transition of all technical activities identified in this task order. As part of the transition, the contractor shall be responsible for:

- Inventory and orderly transfer of all GFP, to include hardware, software, and licenses, Contractor Acquired Government Property, and Government Furnished Information (GFI)
- Transfer of documentation currently in process
- Transfer of all software code in process
- Certification that all non-public DHS information has been purged from any contractor- owned system
- Exchange of accounts to access software and hosted infrastructure components
- Participate in knowledge transfer activities in accordance with the transition plan
- Provide members to and participate in transition management team

Transition support shall commence at least 90 business days prior to expiration of the Task Order. Upon award of a follow-on contract, the incumbent contractor shall work with the new contractor to provide knowledge transfer and transition support, as required by the COR and GPM.

6 DELIVERABLES

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

- Application source code
- Application build scripts
- Test code

- Environment build scripts
- Deployment scripts

All deployed application code shall be checked into the enterprise source code repository. The test code for automated tests is a critical deliverable: USCIS expects good test code coverage (a minimum of 80% unit test code coverage) and effective tests, as these will become part of the regression test suite to be used in future development work as well.

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

The contractor shall submit electronic copies of document deliverables that are indicated in the table below to the CO and COR (and other cc's as may be specified by the CO and/or COR) via e- mail in the format specified. All document deliverables shall be made by close of business (COB) 4:30pm local time Monday through Friday, unless stated otherwise.

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

6.1 Task Order Management Artifacts

The contractor shall provide standard and ad hoc reports such as status briefings that support task order management, as described below:

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

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

6.2 Deliverables Schedule

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

Item	Frequency of Delivery	Acceptable Formats
In-process application code, test code, deployment scripts, build scripts	Continuously, with each build	Code checked into the USCIS code repository
Shippable application code, test code, deployment scripts, build scripts	Continuously, with each commit	Code checked into the USCIS code repository

System Design Document (SDD)	Continuously updated	Wiki
Status Briefings, such as presentations, database extractions, meeting reports, burndown charts, etc.	As directed by the government	MS Word, Excel, Visio, or PowerPoint
Web Services Logs, ICD and other related deliverables	As directed by the government	MS Word, Excel, Visio or PowerPoint
Sprint Review Brief (includes burndown chart, unit testing code coverage, technical debt)	Every two weeks during Sprint Review	PowerPoint, MS Word, Excel, Visio
Staffing Report (includes EOD'd staff and open billets and status)	Weekly for base period and then monthly thereafter	PowerPoint, MS Word, Excel, Visio
Contract Status Report (covers actions completed on each task for time period)	As directed by the government	PowerPoint, MS Word, Excel, Visio
GFE (Make, Model, SN, CIS Number, Contractor Name, Status, Dates) Status	Monthly	Excel
Separation Notification	Within five (5) days of each occurrence to the CO/COR	Email

Table 2: Deliverables Schedule

6.3 Inspection and Acceptance

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

- The government will decide whether to accept functionality delivered after it is demonstrated to a government product owner. The product owner and other stakeholders might provide feedback that requires re-work on the contractor's part. This process follows normal Agile software development practices.
- The government will also periodically evaluate the contractor's code quality, test coverage, test and deployment code quality, security, and so on. Based on these periodic reviews, the government may require rework on the contractor's part. The government expects high quality work that meets standards specified by the government, and does not expect to find significant problems during these reviews.

7 TASK ORDER ADMINISTRATION DATA

7.1 Place of Performance

The principal place of performance shall be at the contractor provided work site for a minimum of 50% of the staff and the key personnel. The government is amenable to remote workers as long as the work is completed efficiently and effectively. The contractor facility shall be in close proximity to the USCIS facility at 111 Massachusetts Ave NW, Washington D.C., not to exceed a distance of 25 commuting miles. Meetings will take place at both the contractor site and USCIS offices in the Washington, D.C. Metropolitan Area, including, but not limited to 20 Massachusetts Avenue, N.W., and 111 Massachusetts Avenue, N.W., Washington DC or other location if indicated by the government. Meetings may also occur at the contractor's work site, especially when close collaboration between stakeholders and the development team is needed. The contractor shall provide workspace, such as a team room, to accommodate up to six Government representatives. One of the six may be a USCIS IV&V tester contractor per development team.

7.2 Hours of Operation

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

7.3 Government Furnished Property (GFP)

Only GFP laptops and cell phones will be issued for those contractors with a compelling need and PIV Cards will be issued and used in performing work on this contract. No personal or company owned storage devices, (thumb drives, DVDs, or CDs) will be used with the GFP. A webinar account, such as Adobe Connect, will be provided to the contractor to facilitate virtual demos and other meetings with stakeholders at various physical locations. Mobile devices may be provided as identified by the COR or GPM.

8 Performance Criteria

VDOS contractor teams will be assessed every 4 weeks and the scorecard evaluation will be discussed with the contractor. The purpose of the scorecard and discussions is to enhance performance. In addition, in the aggregate, the scorecards and discussions will be used partially as a basis for past performance reporting.

The performance criteria will be used in a balanced scorecard type approach. The relative weights of the evaluation categories will be adjusted by the Government based on its experiences, and will be communicated to the contractor after each monthly cycle. The Contracting Officer and contractor will receive a copy of the scorecard. Contractors may provide comments, or responses, to the scorecards to the COR and the Contracting Officer within a week after receipt of the scorecard and rating.

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

- Business Satisfaction. Each feature completed by a contractor team will be evaluated by the Government Product Owner for that team, and possibly by SMEs assigned to the team. At each iteration review, the functionality will be evaluated by a wider audience of Government employees.
- Test Quality and Test Coverage. Because automated tests are a key component of this process, test scripts and code will be treated as deliverables under VDOS. These test

scripts and code will be assessed for their quality and for the extent to which they test the appropriate functions. This evaluation will be performed by the IV&V test team or Government employees.

- Production Performance. The VDOS contractor will be evaluated on the performance of their code in production: its availability, response time, usability, accuracy and lack of defects.
- Collaboration. VDOS contractors will operate within an ecosystem of federal and contractor staff, with multiple contractor teams working in parallel and with constant interaction with USCIS employees. The contractor will be graded based on their willingness, effort, and ability to work collaboratively.
- Productivity. Velocity and story point completion will be measured and compared against historic team averages, the Government will evaluate the value delivered and also to note any unproductive behavior.
- Process and Continuous Improvement. VDOS contractor teams will be assessed on the processes they implement, their conformance to USCIS processes, their conformance with Systems Engineering Life Cycle (SELC) and other required frameworks, and their use of retrospectives to continuously improve these processes.

2. DevOpsSec Team(s) Eagle II Labor Categories and Levels

Key Personnel Program Management Team (Key Personnel)

Team Member	FTE	EAGLE II Labor Category	EAGLE II Level
[redacted]	[redacted]	[redacted]	[redacted]

Team 1

Team Member	FTE	EAGLE II Labor Category	EAGLE II Level
[redacted]	[redacted]	[redacted]	[redacted]

Team 2

Team Member	FTE	EAGLE II Labor Category	EAGLE II Level
[redacted]	[redacted]	[redacted]	[redacted]