

| | | | |
|---------------------------------------|---------------------------------|----------------------------------|--------------------------------|
| 2. AMENDMENT/MODIFICATION NO. 0001 | 3. EFFECTIVE DATE 06/11/2018 | 4. REQUISITION/PURCHASE REQ. NO. | 5. PROJECT NO. (If applicable) |
|---------------------------------------|---------------------------------|----------------------------------|--------------------------------|

| | | |
|---|-------------|---|
| 6. ISSUED BY USCIS Contracting Office Department of Homeland Security 70 Kimball Avenue South Burlington VT 05403 | CODE CIS | 7. ADMINISTERED BY (If other than Item 6) CODE |
|---|-------------|---|

| | | |
|---|---------------|--|
| 8. NAME AND ADDRESS OF CONTRACTOR (No., street, county, State and ZIP Code) | (x) | 9A. AMENDMENT OF SOLICITATION NO. 70SBUR18R00000020 |
| | x | 9B. DATED (SEE ITEM 11) 06/05/2018 |
| | | 10A. MODIFICATION OF CONTRACT/ORDER NO. |
| | | 10B. DATED (SEE ITEM 13) |
| CODE | FACILITY CODE | |

11. THIS ITEM ONLY APPLIES TO AMENDMENTS OF SOLICITATIONS

The above numbered solicitation is amended as set forth in Item 14. The hour and date specified for receipt of Offers is extended. is not extended.
 Offers must acknowledge receipt of this amendment prior to the hour and date specified in the solicitation or as amended, by one of the following methods: (a) By completing Items 8 and 15, and returning _____ copies of the amendment; (b) By acknowledging receipt of this amendment on each copy of the offer submitted; or (c) By separate letter or telegram which includes a reference to the solicitation and amendment numbers. FAILURE OF YOUR ACKNOWLEDGEMENT TO BE RECEIVED AT THE PLACE DESIGNATED FOR THE RECEIPT OF OFFERS PRIOR TO THE HOUR AND DATE SPECIFIED MAY RESULT IN REJECTION OF YOUR OFFER. If by virtue of this amendment you desire to change an offer already submitted, such change may be made by telegram or letter, provided each telegram or letter makes reference to the solicitation and this amendment, and is received prior to the opening hour and date specified.

12. ACCOUNTING AND APPROPRIATION DATA (If required)

13. THIS ITEM ONLY APPLIES TO MODIFICATION OF CONTRACTS/ORDERS. IT MODIFIES THE CONTRACT/ORDER NO. AS DESCRIBED IN ITEM 14.

| | |
|-----------|---|
| CHECK ONE | A. THIS CHANGE ORDER IS ISSUED PURSUANT TO: (Specify authority) THE CHANGES SET FORTH IN ITEM 14 ARE MADE IN THE CONTRACT ORDER NO. IN ITEM 10A. |
| | B. THE ABOVE NUMBERED CONTRACT/ORDER IS MODIFIED TO REFLECT THE ADMINISTRATIVE CHANGES (such as changes in paying office, appropriation date, etc.) SET FORTH IN ITEM 14, PURSUANT TO THE AUTHORITY OF FAR 43.103(b). |
| | C. THIS SUPPLEMENTAL AGREEMENT IS ENTERED INTO PURSUANT TO AUTHORITY OF: |
| | D. OTHER (Specify type of modification and authority) |

E. IMPORTANT: Contractor is not. is required to sign this document and return _____ copies to the issuing office.

14. DESCRIPTION OF AMENDMENT/MODIFICATION (Organized by UCF section headings, including solicitation/contract subject matter where feasible.)

myUSCIS
 EAGLE II FC1 Unrestricted
 RFP submission due date is June 21, 2018 @ 2PM EST

Period of performance will be a 9 month base, that includes a 120 day transition period, with two 12 month options from the date the Notice to Proceed (NTP) is issued.

DO/DPAS Rating: NONE
 Continued ...

Except as provided herein, all terms and conditions of the document referenced in Item 9 A or 10A, as heretofore changed, remains unchanged and in full force and effect.

| | |
|---|--|
| 15A. NAME AND TITLE OF SIGNER (Type or print) | 16A. NAME AND TITLE OF CONTRACTING OFFICER (Type or print) Chad R. Parker |
| 15B. CONTRACTOR/OFFEROR (Signature of person authorized to sign) | 15C. DATE SIGNED |
| | 16B. UNITED STATES OF AMERICA (Signature of Contracting Officer) |
| | 16C. DATE SIGNED |

CONTINUATION SHEET

REFERENCE NO. OF DOCUMENT BEING CONTINUED
70SBUR18R00000020/0001

PAGE OF
2 63

NAME OF OFFEROR OR CONTRACTOR

| ITEM NO. (A) | SUPPLIES/SERVICES (B) | QUANTITY (C) | UNIT (D) | UNIT PRICE (E) | AMOUNT (F) |
|-----------------|---|-----------------|-------------|-------------------|---------------|
| | Delivery Location Code: HQOIT Department of Homeland Security US Citizenship & Immigration Svcs Office of Information Technology 111 Massachusetts Ave, NW Suite 5000 Washington DC 20529 FOB: Destination Change Item 0001 to read as follows (amount shown is the obligated amount): Base period of performance: 5 months from the end of Transition In CLINs 0006 and 0007. | | | | |
| 0001 | Program Management (Fixed Price) As described in the SOW section 2 Change Item 0002 to read as follows (amount shown is the obligated amount): | 5 | MO | | |
| 0002 | Technical Support and Agile Teams (Fixed Price) As described in the SOW section 2 Change Item 0003 to read as follows (amount shown is the obligated amount): | 5 | MO | | |
| 0003 | Government Directed Travel: As described in the SOW section 6 ODC Cost Reimbursement CLIN Not to exceed \$25,000.00 Change Item 0004 to read as follows (amount shown is the obligated amount): | 1 | LO | | |
| 0004 | Optional CLIN: Additional Agile Team (Fixed Price) As described in the SOW section 2 (Team of 10 FTEs) (Option Line Item) Change Item 0005 to read as follows (amount shown is the obligated amount): | 5 | MO | | |
| 0005 | Optional CLIN: Additional Agile Team (Fixed Price) As described in the SOW section 2 Continued ... | 5 | MO | | |

CONTINUATION SHEET

REFERENCE NO. OF DOCUMENT BEING CONTINUED
70SBUR18R00000020/0001

PAGE OF
3 63

NAME OF OFFEROR OR CONTRACTOR

| ITEM NO. (A) | SUPPLIES/SERVICES (B) | QUANTITY (C) | UNIT (D) | UNIT PRICE (E) | AMOUNT (F) |
|-----------------|---|-----------------|-------------|-------------------|---------------|
| | (Team of 10 FTEs) (Option Line Item) 0 Days After Award | | | | |
| | Change Item 0006 to read as follows (amount shown is the obligated amount): Transition period of performance: 4 months from the date the NTP is issued | | | | |
| 0006 | Program Management Transition In (Fixed Price) As described in the SOW section 3 | 4 | MO | | |
| | Change Item 0007 to read as follows (amount shown is the obligated amount): | | | | |
| 0007 | Technical Support and Agile Teams Transition In (Fixed Price) As described in the SOW section 4 | 4 | MO | | |
| | Change Item 1001 to read as follows (amount shown is the obligated amount): Option I period of performance: 12 months from the end of the base period. | | | | |
| 1001 | Option I: Program Management (Fixed Price) As described in the SOW section 2 (Option Line Item) 0 Days After Award | 12 | MO | | |
| | Change Item 1002 to read as follows (amount shown is the obligated amount): | | | | |
| 1002 | Option I: Technical Support and Agile Teams (Fixed Price) As described in the SOW section 2 (Option Line Item) | 12 | MO | | |
| | Change Item 1003 to read as follows (amount shown is the obligated amount): | | | | |
| 1003 | Option I: Government Directed Travel As described in the SOW section 6 | 1 | LO | | |
| | Continued ... | | | | |

CONTINUATION SHEET

REFERENCE NO. OF DOCUMENT BEING CONTINUED
70SBUR18R00000020/0001

PAGE OF
4 63

NAME OF OFFEROR OR CONTRACTOR

| ITEM NO. (A) | SUPPLIES/SERVICES (B) | QUANTITY (C) | UNIT (D) | UNIT PRICE (E) | AMOUNT (F) |
|-----------------|--|-----------------|-------------|-------------------|---------------|
| | ODC Cost Reimbursement CLIN Not to exceed \$60,000.00 (Option Line Item) 0 Days After Award | | | | |
| | Change Item 1004 to read as follows (amount shown is the obligated amount): | | | | |
| 1004 | Option I Optional CLIN: Additional Agile Team (Fixed Price) As described in the SOW section 2 (Team of 10 FTEs) (Option Line Item) 0 Days After Award | 12 | MO | | |
| | Change Item 1005 to read as follows (amount shown is the obligated amount): | | | | |
| 1005 | Option I Optional CLIN: Additional Agile Team (Fixed Price) As described in the SOW section 2 (Team of 10 FTEs) (Option Line Item) 0 Days After Award | 12 | MO | | |
| | Change Item 2001 to read as follows (amount shown is the obligated amount): | | | | |
| | Option II period of performance: 12 months from the end of the Option I period of performance. | | | | |
| 2001 | Option II: Program Management (Fixed Price) As described in the SOW section 2 (Option Line Item) 0 Days After Award | 12 | MO | | |
| | Change Item 2002 to read as follows (amount shown is the obligated amount): | | | | |
| 2002 | Option II: Technical Support and Agile Teams (Fixed Price) As described in the SOW section 2 (Option Line Item) 0 Days After Award | 12 | MO | | |
| | Continued ... | | | | |

NAME OF OFFEROR OR CONTRACTOR

| ITEM NO. (A) | SUPPLIES/SERVICES (B) | QUANTITY (C) | UNIT (D) | UNIT PRICE (E) | AMOUNT (F) |
|-----------------|--|-----------------|-------------|-------------------|---------------|
| 2003 | Change Item 2003 to read as follows (amount shown is the obligated amount): Option II: Government Directed Travel As described in the SOW section 6 ODC Cost Reimbursement CLIN Not to exceed \$60,000.00 (Option Line Item) 0 Days After Award | 1 | LO | | |
| 2004 | Change Item 2004 to read as follows (amount shown is the obligated amount): Option II Optional CLIN: Additional Agile Team (Fixed Price) As described in the SOW section 2 (Team of 10 FTEs) (Option Line Item) 0 Days After Award | 12 | MO | | |
| 2005 | Change Item 2005 to read as follows (amount shown is the obligated amount): Option II Optional CLIN: Additional Agile Team (Fixed Price) As described in the SOW section 2 (Team of 10 FTEs) (Option Line Item) 0 Days After Award 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. SOW Attachment # 1: myUSCIS System Integrations - Diagram 3. SOW Attachment #2: Current Pipeline - Diagram 4. SOW Attachment #3: The current technical stack Continued ... | 12 | MO | | |

CONTINUATION SHEET

REFERENCE NO. OF DOCUMENT BEING CONTINUED
70SBUR18R00000020/0001

PAGE OF
6 63

NAME OF OFFEROR OR CONTRACTOR

| ITEM NO. (A) | SUPPLIES/SERVICES (B) | QUANTITY (C) | UNIT (D) | UNIT PRICE (E) | AMOUNT (F) |
|-----------------|--|-----------------|-------------|-------------------|---------------|
| | <p>& tools</p> <p>5. Attachment #4: myUSCIS Government Sample Staffing Mix and CLIN Structure (provided in PDF and Excel Spread Sheet)</p> <p>6. Attachment #5: Questions and Answers</p> <p>Part IV - Solicitation Provisions/Instruction/Evaluation: 1. Solicitation Provisions/Instruction/Evaluation</p> | | | | |

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

| | |
|--|------------|
| 52.204-19 Incorporation by Reference of Representations and Certifications | (Dec 2014) |
| 52.224-3 Privacy Training | (Jan 2017) |
| 52.232-39 Unenforceability of Unauthorized Obligations | (Jun 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 **30** days; provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least **60** days before the task order expires. The preliminary notice does not commit the Government to an extension.

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

(c) The total duration of this contract, including the exercise of any options under this clause, shall not exceed **33 months**.

(End of clause)

52.252-4 Alterations in Contract

(Apr 1984)

Portions of this contract are altered as follows: Use of the word “contract” is understood to mean “task order” whenever such application is appropriate.

(End of clause)

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

3052.203-70 Instructions for Contractor Disclosure of Violations.

(SEP 2012)

When making a written disclosure under the clause at FAR 52.203-13, paragraph (b)(3), the Contractor shall use the Contractor Disclosure Form at <http://www.oig.dhs.gov> and submit the disclosure electronically to the Department of Homeland Security Office of Inspector General.

The Contractor shall provide a copy of the disclosure to the Contracting Officer by email or facsimile on the same business day as the submission to the Office of Inspector General. The Contractor shall provide the Contracting Officer a concurrent copy of any supporting materials submitted to the Office of Inspector General.

(End of clause)

3052.205-70 Advertisements, Publicizing Awards, and Releases.

**ALTERNATE I
(SEP 2012)**

- (a) The Contractor shall not refer to this contract in commercial advertising or similar promotions in such a manner as to state or imply that the product or service provided is endorsed or preferred by the Federal Government or is considered by the Government to be superior to other products or services.

All advertisements, releases, announcements, or other publication regarding this contract or the agency programs and projects covered under it, or the results or conclusions made pursuant to performance, must be approved by the Contracting Officer. Under no circumstances shall the Contractor, or anyone acting on behalf of the Contractor, refer to the supplies, services, or equipment furnished pursuant to the provisions of this contract in any publicity, release, or commercial advertising without first obtaining explicit written consent to do so from the Contracting Officer.

(End of clause)

3052.215-70 Key Personnel or Facilities

(Dec 2003)

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

(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 (SOW), 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 REGARDING AGILE TEAMS

The Government's expectation is that the Contractor's Agile teams will continuously provide at least 10 FTEs of IT professionals performing the roles described in the SOW, and that each team will work effectively within itself and collaboratively with the Government to achieve the Government's needs as generally described in the SOW. The Contractor's inability to continuously provide the expected FTEs for a team may put achievement of Government objectives at risk of non-fulfillment and may result in termination of the task order for the Contractor's default. The government will allow (i) contractors to manage a smooth transition of individuals in/out as required to support evolving skills needs on the contract and (ii) participation by team members on a part-time basis based on program needs so long as the sum of the team is continuously at 10 FTEs.

EXPECTATION OF CONTRACTOR PERSONNEL

The Government expects competent, productive, qualified IT professionals to be assigned to the Agile teams. The Contracting Officer, by written notice to the Contractor, may require the Contractor to remove any employee from the work if the Contracting Officer deems that employee not to be competent, productive, or qualified.

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 |
|------------------|------------|-------------|-------------------------|
| Laptop computer | 1 | EA | \$ 4,500 |
| PIV Card | 1 | EA | \$ 500 |
| Cell Phone | 1 | EA | \$ 1,000 |

(b) The Government will issue this equipment only to contractor employees that have a successful EOD.

(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 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 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)

Full contract performance shall begin commencing on the date specified by the Contracting Officer in the Notice to Proceed directive.

(a) Performance of the work requires unescorted access to Government facilities or automated systems, and/or access to sensitive but unclassified information. The Security Requirements below applies. The Contractor is responsible for providing employees who will receive favorable entry-on-duty (EOD) decisions and suitability determinations. A Government decision not to grant a favorable EOD decision or suitability determination, or to withdraw or terminate such decision or termination, shall not excuse the Contractor from performance of obligations under this task order.

(b) The Contractor may submit background investigation packages upon issuance of the task order, so that it has adequate employees ready for the time when the Government issues the notice to proceed.

(c) The Government intends to issue a notice to proceed between 30 and 60 days after task order award.

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 all contractor staff.

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. ACCESSIBILITY REQUIREMENTS (SECTION 508)

Accessibility Requirements (Section 508)

Section 508 of the Rehabilitation Act, as amended by the Workforce Investment Act of 1998 (P.L. 105-220) requires that when Federal agencies develop, procure, maintain, or use information and communications technology (ICT), it shall be accessible to people with disabilities. Federal employees and members of the public who have disabilities must have access to and use of information and data that is comparable to Federal employees and members of the public without disabilities. All products, platforms, and services delivered as part of this work statement that are by definition ICT or contain ICT shall conform to the Revised 508 Standards, which are located at 36 C.F.R. § Appendices A, C, and D, and available at <https://www.gpo.gov/fdsys/pkg/CFR-2017-title36-vol3/pdf/CFR-2017-title36-vol3-part1194.pdf>.

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

Section 508 Applicable EIT Accessibility Standards

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

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

36 CFR 1194.24 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. Agencies cannot claim a product as a whole is not commercially available because no product in the marketplace meets all the standards. If products are commercially available that meet some but not all of the standards, the agency must procure the product that best meets the standards. When applying this standard, all procurements of EIT shall have documentation of market research that identify a list of products or services that first meet the agency business needs, and from that list of products or services, an analysis that the selected product met more of the accessibility requirements than the non-selected products as required by FAR 39.2. Any selection of a product or service that meets less accessibility standards due to a significant difficulty or expense shall only be permitted under an undue burden claim and requires authorization from the DHS Office of Accessible Systems and Technology (OAST) in accordance with DHS MD 4010.2.

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

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 (OSIPSD).

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 OSIPSD 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>

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

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

(b) **Security Training Requirements**.

(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

Statement of Work myUSCIS

Procurement Sensitive – See FAR 3.104

This document contains proprietary information related to the conduct of a Federal agency procurement, the disclosure of which is restricted by Section 27 of the Office of Federal Procurement Policy Act (41 U.S.C. 423). The unauthorized disclosure of such information may subject both the discloser and recipient of the information to contractual, civil, and/or criminal penalties as provided by law.

1. Scope of Work

1. The Department of Homeland Security (DHS), United States Citizenship and Immigration Services (USCIS), Office of Information Technology (OIT) requires support developing myUSCIS. The vendor will be required to provide services in the development of new and enhancement of existing capabilities (myUSCIS) that make it easy for users to understand and navigate the immigration process, apply for benefits online, view information about their cases, respond to requests for additional information and contact USCIS for support.
2. myUSCIS will continue to provide the public facing front end for the applicants and petitioners. The back end case management systems are integrated with myUSCIS and may vary. The back end case management systems themselves are not the responsibility of the myUSCIS contractor, but integration and collaboration with these systems and teams is required. myUSCIS does not store the data once it has been submitted to the case management system. These case management systems may include among others, Claims 3, Claims 4 and ELIS. Making new forms available involves not only the UI but also the various integrations with downstream case management systems and other systems that contain historical benefits information utilizing services, RESTful APIs and microservices such as the draft case and payment services. Currently five USCIS forms are available for online filing via myUSCIS. The application data from these first five forms (data from the applicant forms) resides in one of the USCIS case management systems known as ELIS.
3. USCIS requires Agile software development services to support our user community. The myUSCIS user community includes applicants, petitioners, legal representatives, sponsors or community based organizations that assist applicants and/or petitioner with the immigration process. USCIS requires vendor design services that focuses on user needs, user research, and ethnographic research, as is a critical aspect of the success of the myUSCIS toolset. Support for developing new and maintaining the existing iOS and Android USCIS Civics Test Study Tools mobile application is also required. Ethnographic researchers works closely with user researchers and designers to observe people from different cultures so that a robust and effective user experience is provided. Immigration is the focus, and thus, people from different cultures are our users. The Ethnographic specialization helps our user research teams put themselves in the shoes of those applicants, without influencing them, in order to understand what is helpful so that the user experience is as positive and user friendly as possible

4. This requires clear, continuous and effective communication and collaboration between the product owner and the project team to research, design, architect, engineer, document, and maintain the myUSCIS mobile responsive web applications and mobile application. No sensitive data or PII is shared between the mobile apps and the listed systems. The current FISMA level across the myUSCIS systems is Moderate.
5. These features are developed using Agile methodology in an iterative fashion using continuous deployment pipelines in Amazon Web Service (AWS). Our immutable AWS infrastructure enables zero downtime deployments of new features, enhancements and bug fixes immediately after they are complete and tested. The AWS infrastructure will evolve along and myUSCIS has evolving requirements as well, therefore, the contractor must leverage Agile best practices in software development; including but not limited to, human-centered design, test driven development, open source code, continuous integration, pair programming, extensible infrastructure.
6. USCIS is focused on the goal of eProcessing by 2020, and since we still have over 100 forms to bring online.. An implementation plan is not currently available for the eProcessing, however, USCIS may need additional services (optional CLINS) to meet the deadline set forth by the USCIS Leadership. Those additional services are expected to be completed under the optional CLINs for additional teams
7. The contractor shall provide the Government with four Agile teams during the base period, and if exercised 2 additional optional teams. The contractor shall provide the Government with 5 Agile teams during each of the option periods, and if exercised 2 additional optional teams. (*Reference Sample Staffing Mix Attachment #4*). Additional teams are required through optional CLINS to allow the Government to receive additional support.
8. Additional SOW attachments are as follows:
 - a. SOW Attachment # 1: The System Integrations Diagram
 - b. SOW Attachment #2: The Current Pipeline Diagram
 - c. SOW Attachment #3: The Current Technical Stack & Tools

2. Tasks

Program Management (CLIN 0001, 1001, 2001)

1. The contractor shall provide program management and administration support in managing the technical tasking in this SOW. The PM role is not expected to increase as optional CLINs are exercised.
 - a. Administrative support tasks include, but not limited to, meeting logistics and coordination, maintaining contractor EOD submission paperwork, contractor provisioning requests for email, PIV card, GFE, exit and transfer paperwork, and documentation.
 - b. Program management support will include oversight of the program, team communication, performance, personnel, financials and reporting.
 - i. The contractor will provide a program manager (PM) who is responsible for all aspects of the program management function.
 1. The PM will be the primary interface with the Government.

2. The PM shall be required to attend a bi-weekly meeting to discuss the program performance and any issues or upcoming initiatives.
3. The PM is responsible for formulating, and delivering an action plan to correct identified issues or initiatives.
4. The contractor PM shall prepare and deliver a monthly presentation to Customer service and Public Engagement Directorate (CSPED) and OIT detailing completed and upcoming work.
5. The PM shall ensure that all deliverables are provided in a timely manner. The PM shall support security processing, which is the interface with Government Office of Security and Integrity (OSI) through the COR on all security matters, to include physical, personnel, and protection of all Government information and data accessed by the contractor.
6. Agile Scope coordination will occur through (i) agreement on new work scope and size of features to be developed at the start of a given Release or Sprint, (ii) validation that mobilized team capacity can accept the new scope, and (iii) confirmation that acceptance criteria is coordinated with the Program Manager.

Technical Support (Supports the Agile Development Teams CLIN 0002, 1002, 2002)

In addition to the agile teams the contract structure requires a level of technical support across all of the Agile development teams in the form of advisors or leads. Technical lead roles are not expected to increase as optional CLINs are exercised.

Design Lead Efforts

The Design Lead is responsible for executing User Experience (UX) strategies and creating products that enable lawful immigration. This person must be proficient in user centered design, how people interact effectively with websites and digital tools and proficiency in the latest design methods and technology trends.

Design Lead responsibilities include:

1. Manage the design team as well as design related planning, prioritization and decision making.
2. Lead and participate in design studios and strategy sessions that leverage ethnographic user research and innovative design methods with the goal of informing design improvements that improve the user experience.
3. Translate user needs into concepts, personas, user journeys, information architecture, user flows, wireframes and visual design prototypes using design tools such as Sketch, Mural, Adobe Creative Suite, and InVision.
4. Conduct user research and usability testing, and translate those results into designs that will improve products in an iterative fashion.
5. Collaborate effectively with USCIS Product Managers, Software Developers, and USCIS Leadership to articulate the design vision, tradeoffs and decisions.

6. Partner with software developers and product managers to ensure that designs are properly implemented, regularly tested with users and iteratively improved.
7. Work with USCIS Office of Communications (OCOMM) to adhere to USCIS and DHS brand guidelines.
8. Collaborate with DHS Trusted Testers and Office of Accessible Systems & Technology (OAST) to ensure that designs are Section 508 complaint for accessibility.
9. Balance user needs with product owner priorities and technical feasibility.
10. Provide plain language content strategy to facilitate an easy to understand user experience that simplifies a complex process for users who may not be native English speakers. The design lead will be responsible for developing clear easy to understand language. When necessary another team will translate content if required.

Technical Lead Efforts

The Technical Lead is responsible for empowering cross-functional teams to meet the functional requirements set forth by the USCIS Product Management Team. The Technical Lead must have strong verbal and written communication skills and must collaborate effectively with Product Owners, developers and designers to build easy to use, software applications using a variety of leading-edge technologies.

Technical Lead responsibilities include:

1. Responsible for communicating technical options, and associated tradeoffs and risks, with the USCIS Product Management team and USCIS Leadership.
2. Experienced in public facing web application development and iOS/Android application development.
3. Demonstrates knowledge and understanding of industry trends, innovative technologies, software development methods and tools in order to continuously improve and evolve the product architecture, user experience, and Agile development and DevOps practices.
4. Foster the use of Agile practices within teams to enable delivery of deployable software within specified times.
5. Actively participate in design sessions, sprint ceremonies and cross functional and integration team meetings.
6. Provide guidance and oversight of testing practices and code reviews, and ensure the security and integrity of the code base and product.
7. Collaborate with team members and integration partners to develop new features as well as to troubleshoot, debug, and resolve-issues in all environments.

DevOps Lead Efforts

The DevOps Lead supports the myUSCIS applications which are currently hosted in the AWS cloud. The DevOps Lead supports the existing continuous integration/continuous delivery (CI/CD) pipelines and researches ways to continuously improve them while ensuring high quality software solution delivery using modern, secure, scalable, stable environments.

DevOps Lead responsibilities include:

1. Responsible for the effectiveness and continuous improvement of all the DevOps processes, practices and activities.
2. Maintain and improve software solutions delivery across multiple Agile teams.

3. Maintain CI/CD pipelines using configuration management best practices for developing and deploying web applications.
4. Familiarity with the use of automated configuration management, auto-scaling, containers, REST services, AWS apps technologies and AWS IaaS Technologies
5. Research innovative tools that will improve the application infrastructure while reducing costs.
6. Implement processes and scripts that will automate manual tasks related to software development, testing and deployment to ensure rapid delivery of quality solutions.
7. Research, develop and enhance DevOps monitoring tools and processes to minimize downtime and maximize transparency and system stability.
8. Manage several integrated environments with multiple systems including connection and security configurations
9. Monitor and maintain the application and immutable infrastructure to ensure performance, stability and security. (Immutable infrastructure is an approach to managing services and software deployments on IT resources wherein components are replaced rather than changed. An application or services is effectively redeployed each time any change occurs)
10. Collaborate with Product Managers, developers and integration partners to debug applications and scripts to resolve defects and performance issues.
11. Apply regular, routine security and OS patches as required.
12. Work with the USCIS Information Systems Security Officer (ISSO) to oversee the performance of security scans with each build, remediate scan findings and support ongoing authorization and improved security posture.
13. Support implementation and testing of DHS infrastructure change requests as required.

Agile Development Teams (CLIN 0002, 1002, 2002)

Modern Technology & Techniques

1. The contractor shall continue to improve upon the existing myUSCIS web and Civics Test Study Tools mobile applications in order to further enhance the user experience.
2. The contractor teams shall create modern digital services for myUSCIS that use modern technical stacks.
3. The contractor's support and solutions are required to align with the U.S. Digital Services Playbook <https://playbook.cio.gov>. The contractor shall be familiar with the concepts in each play and the contractor shall implement them in its approaches and support for USCIS.
4. The contractor shall participate in USCIS's Agile methodologies and related ceremonies (e.g. backlog grooming, sprint planning, daily stand-ups, sprint review, sprint retrospective, and scrum of scrums).
5. The contractor will be responsible for the activities associated with design, development, configuration, customization and deployment of solutions. Once deployed, the contractor shall provide production support and enhancements as required.
6. The contractor shall provide modern digital services that use development and operations (DevOps) techniques that embrace cloud based, scalable architecture, immutable infrastructure, automated testing and continuous integration and continuous deployment.

7. The contractor shall deliver secure and tested mobile and web designs and applications using automated testing frameworks that utilize services, microservices and containers.
8. The contractor shall provide support as USCIS builds brand new systems, integrates with other systems and enhances existing systems. The contractor shall provide support for new tools, technologies and programming languages as they emerge.
9. The contractor shall work closely with the Government IT program managers from OIT and product owners from CSPED to conduct user research, create, groom, develop, design, prioritize and test user stories that will serve as the foundation for the development work. The product management team from CSPED provides guidance on product vision, business requirements and priority of work as well as validation that user stories meet the acceptance criteria for each story. The OIT program managers provide technical oversight.
10. The contractor shall use Agile methods and modern tools and techniques to design, develop, deploy, and maintain solutions for myUSCIS and related systems. The contractor shall provide support that includes user research, UX design, user interface prototyping, application development, systems integration, data analytics, program management, DevOps support, testing, validation and deployment into cloud environments.
11. The Contractor must provide a DHS OAST Trusted Tester certified to current test standards for each team of one or more developers that creates Information and Communications Technology (ICT), or content to be hosted on ICT, within 90 days of award. When standards change and re-certification is required by DHS OAST then the Contractor must ensure that all Trusted Testers re-certify within 90 days of training availability.
12. The Contractor must provide a quarterly report that lists the contract name, number, and COR with each Trusted Tester's name, certification level, certification date, certification number, E-mail address, phone number, and supported projects to the COR and USCIS Section 508 Coordinator. This report must also be provided within 10 working days of any change in the Trusted Tester population.

Maintenance

1. Maintenance related activities include but are not limited to remediating defects as prioritized by the product owners, system monitoring for performance and identifying bottlenecks, troubleshooting issues with networking and integration teams, OS and security patches, software upgrades, responding to security scan findings and remediating security Plan of Action and Milestones (POA&Ms).
2. Maintenance tasks related to the website infrastructure including all previously developed forms and features as well as the USCIS Civics Test Study Tools mobile app. There is also an internal custom component to the myUSCIS system called Command Center that is used by internal USCIS employees to manage content and set feature toggles.

Design

1. Design includes, user research, user experience, user interface, visual design (mobile & responsive), ethnographic research, content strategy and plain language strategy, and collaboration with product owners.

2. The contractor shall perform user research to discover user needs using methods such as design studios, user interviews, and usability testing. The contractor shall work with USCIS in order to determine the best location for usability testing sessions and identify and recruit users to participate.
3. The contractor shall deliver a research plan prior to beginning the sessions, and the contractor shall provide detailed findings in the form of mock up prototypes, presentations after conducting the sessions.
4. The contractor's design and development staff shall work together in order to transform user needs into myUSCIS features that will improve the usability of the applications.
5. The contractor shall produce designs that adhere to the existing myUSCIS style guide (provided after award) and the contractor shall consider the overall website and brand as they create new and enhance existing features as part of a cohesive and unified user experience.
6. The contractor shall ensure that they successfully achieve the definition of done by working with internal USCIS stakeholders on issues such as 508 compliance and security guidelines. All content and designs created by the contractor shall be section 508 compliant for accessibility.

Mobile

1. The Civics Test Study Tools mobile app is currently available in the Apple App Store and the Google Play Store. This hybrid mobile app built in react native is used by people seeking citizenship as a tool to help them study for their civics test during their citizenship interview.
2. The contractor shall maintain this existing mobile application as required.
3. The contractor shall support the design and development of new mobile applications as prioritized by the Federal CSPED product owner/product management team. New mobile applications are crucial in achieving the goal of improving usability and accessibility and should be available in Apple App store and Google Play Store. Mobile applications shall be in compliance of mobile security guidelines and 508 compliant guidelines. GFE mobile devices, both iOS and Android, are available for testing.
4. The myUSCIS website is a mobile responsive, cloud-based solution and the contractor shall support enhancing and maintaining it as a responsive web application, as well as its infrastructure and its various integration points.

Agile Development

1. Development/architecture includes, enterprise architecture support, Ruby on Rails, React, React-Native, Python and Java developers, responsive web application architecture and development, development using a variety of open source tools and languages, native and hybrid mobile application architecture and development, and Front-end UI development including rapid prototyping capabilities.
2. The contractor shall support the use of Agile methods to iteratively enhance existing functionality and design and develop new functionality that will allow users to apply for additional immigration benefits, view and receive updates on the status of their applications, and increase communication channels with USCIS.
3. The contractor shall deliver high quality, production-ready functionality in an incremental fashion using Agile development practices and methods. The contractor

shall conduct scrum/Kanban ceremonies which may include but are not limited to grooming, review, planning, and retrospective.

4. The contractor shall deliver all requested documents including, but not limited to, lifecycle management gate review documents, status reports, metrics reports, process flows, presentations, minutes, flow charts, designs, trip reports and research plans.
5. Ruby on Rails and React are used for development and the frameworks used are MVC and Spring for public facing components and the backend integrations. APIs are used to surface data to the front end and share data with the backend.
6. Currently, myUSCIS uses Atlassian's Jira and Confluence to document, plan, track and manage the development and the overall program. The Confluence wiki contains a plethora of information about the project, processes, structure, research, resources etc. This resource will be a key tool in guiding transition activities. The contractor shall update and maintain a central document repository so that information remains relevant and easy to locate. This archive of information is crucial to the management of the program.

DevOps

1. DevOps includes system architecture, development and administration, automated test and evaluation, AWS tools and infrastructure, and continuous integration and continuous deployment pipelines.
2. DevOps is an integral part of supporting myUSCIS Amazon Web Services cloud-based, public facing website. The contractor shall support the AWS toolsets and shall monitor and maintain multiple environments with continuous integration and continuous delivery pipelines that utilize automated builds, automated tests and static analysis.
3. The contractor shall provide proactive monitoring and analysis to ensure that the system and its interfaces are available and functioning properly.
4. The contractor shall monitor and support automated performance testing to ensure responsiveness and stability of the application, and the systems that are integrated with it, are maintained.
5. The contractor shall work with the USCIS Information Systems Security Officer (ISSO) in order to remediate any findings from the regular security scans that USCIS performs on the system. The ISSO is not a member of the myUSCIS contractor team; rather they support the Information Security Division (ISD) and provide security oversight.
6. The contractor shall update and assist with updating the required security documentation for the project, including but not limited to the System Security Plan. The current architecture uses Akamai's CDN (content delivery network) services globally across USCIS, Nginx and Passenger for handling web requests, Sidekiq for background processing jobs, Redis for caching and Postgres databases. Most of the web applications are deployed in containers.
7. myUSCIS is enrolled in the Team Managed Deployment Program (TMD) at USCIS. TMD means that the contractor deploys to production autonomously using fully automated CI/CD pipelines. The myUSCIS team uses feature toggles and blue green deployments to reduce risk and control access to features as they are being developed.
8. DevOps resources can either be co-located with the greater development teams or work entirely remotely, as long as team collaboration, coordination, velocity, and product quality is not negatively impacted.

Data Science

1. Contractors shall analyze large amounts of data to inform/identify new features that will improve upon existing application functionality for an enhanced user experience. The contractor shall provide data solution architecture, data engineering, data science, and data analysis support that analyzes, synthesizes, and integrates large quantities of structured and unstructured data that will be used to enhance the tools and features of the myUSCIS applications. These features will better inform applicants and representatives about details such as their immigration journey, the status of their cases and the duration of the overall application process.
2. The contractor shall use this data to develop and improve tools that will provide answers to frequently-asked and case specific questions. The Contractor shall be able to use a combination of supervised and unsupervised machine learning algorithms, predictive models, and statistical algorithms in order to provide insights into USCIS datasets. USCIS may use these insights to improve operational decisions and enhance the USCIS external user experience. The contractor shall continuously reevaluate the collection and analysis of data against changing agency needs.
3. Data Science includes, Google Analytics and metrics, statistical analysis, machine learning and natural language processing, and data science, analytics, modeling and integration.

Support activities that the contractor shall provide may include the following:

- User research and design sessions with actual applicants, representatives and community based organizations that are in the process of applying for benefits. These sessions will drive the design and creation of features that will improve usability and understanding for our users. The contractor shall plan, organize, facilitate, and collect data from focus group and research/usability testing sessions. The sessions shall be held several times each year and each event may have multiple sessions.
 - The Government will select the geographical locations within the United States, and the sessions will be held with users who seek to obtain benefits.
 - The Government will provide the contractor with an electronic data list of USCIS customers and e-mail addresses from which users will be selected to participate in the sessions. The contractor shall contact the users by email and telephone to schedule their participation. The contractor shall provide a moderator's guide that outlines the questions that will be asked. The contractor shall use the data collected to produce reports following each session. The report shall include the methodology used to collect the data and a detailed description of the observations and outcomes.
- Expansion of the myUSCIS experience by designing, developing, and deploying additional tools for public users of many types, including tools that allow users to receive up to date information about their immigration journey. Based on user research, these tools will be developed but could include tools such as:
 - Proactive notifications to keep benefit seekers informed as to the status and next steps associated with their applications

- An eligibility tool to help customers understand which benefits are available to them
- Additional mobile applications for iOS and Android users since the majority of our users have mobile devices
- Support the overall eProcessing initiative:
 - Online filing of all immigration forms and benefits as prioritized by USCIS
 - Integration with the USCIS prescribed identity verification system which will provide applicant history and will inform actions that can be taken by the authenticated user
 - Additional profile management capabilities to support more efficient completion of additional benefits applications
 - Expansion of the current account experience to include, but not limited to representative-based accounts, corporate based accounts and family based accounts
 - Integration with the USCIS content management services and person-centric services to provide a more robust account experience for authenticated users
- Data Science and analytics:
 - Expand upon the existing models to estimate how long it will take to process USCIS benefits forms and to present relevant information to users about their immigration journey
 - Develop and deploy personalized processing times models for additional benefits forms as prioritized by USCIS
 - Add integration points for the intelligent automated help agent to connect with external applications or data sources, in order to increase its effectiveness and accuracy
 - Create and implement scrubbing strategies to ensure unstructured data is appropriate to present to the end user
 - Analyze customer data and biometrics to identify key data points for confirming a customer's identity
 - Analyze, validate, and create an ETL process to transition from a transaction based model to a customer centric model

Optional Teams (CLINs 0004 & 0005, 1004 & 1005, 2004 & 2005)

Due to the urgency and criticality associated with the eProcessing initiative, the Government may exercise optional CLINS to add additional Agile development teams. The optional teams shall perform the same functions as the Agile development teams under CLINs 0002, 1002, and 2002.

3. Program Management Transition (CLIN 0006)

The contractor shall provide program management and administration support in managing the technical tasking in this SOW. Administrative support shall include tasks such as meeting logistics and coordination, contractor EOD submission paperwork, contractor provisioning requests for email, PIV card, GFE, exit and transfer paperwork, documentation etc. The program manager is responsible for developing and providing the transition plan. The program manager

will facilitate the mix of labor sufficient to support transition. The program manager will be the primary interface with the Government to support a smooth transition.

4. Transition (CLIN 0007)

1. The contractor shall participate in transition activities. The contractor shall develop a transition plan that shall be used to allow the current contractor to complete existing work and to transition ongoing work over to the new contractor.
2. Transition-In Period (120 days)
3. Within 15 days after the Notice to Award, the contractor shall develop and deliver to the Government a transition plan, allowing no more than 120 days for an orderly transition.
4. The transition-in period shall begin with the receipt of a notice to proceed from the contracting officer.
5. The contractor shall execute its transition plan and work closely with the incumbent contractor or the Government to ensure uninterrupted contract support.
6. Transition-in activities shall also include contractor attendance at program reviews, participation in working groups, briefings, and on-site communications. Proposed staff levels during the transition in period shall be included within the transition plan.
7. The contractor shall exercise its best efforts and cooperation to effect an orderly and efficient transition to a successor. Negotiate in good faith a plan with a successor to determine the nature and extent of phase-in services required.

Transition Plan

The contractor shall work with senior management as required to support the planning of transition activities within the organization. The contractor's Transition Plan shall include the procedures for the transition-in and transition out.

The Transition Plan should assume a 120 day time frame in 3 phases.

- Phase 1 (45 days): The incoming vendor will conduct on-boarding activities while the outgoing vendor remains responsible for delivery of the IT Services. To include transferring responsibilities.
- Phase 2 (30 days): Consists of the outgoing vendor continuing to provide service from the "Drivers Seat" while the incoming vendor shadows in the passenger seat and prepares for transition.
- Phase 3 (45 days): Consists of the incoming vendor assuming responsibility for the delivery of IT services while the outgoing vendor executes ramp down activities.

At a minimum, the transition plan shall be inclusive of the transition of the documentation, operating procedures and other resources, including but not limited to, software, devices, equipment, environments and systems from the current incumbent contractor or the Government.

At a minimum, the transition plan shall address transition communication which shall include:

- A transition team directory
- A stakeholder's matrix
- A schedule for weekly transition meetings
- A proposed template and schedule for delivery of transition status reports

- An escalation sequence for Government questions or issues
- Hiring status
- Transition risk and planned mitigation
- Reports on production bugs and resolutions
- Perform project management coordination and communication

Transition-Out (Executed through FAR 52.237-3 Clause – NOT PRICED)

5. Place of Performance

1. The primary place of performance for this task order is the contractor's facility; therefore, contractor site rates are required under this task order. If required, the contractor shall provide work space in the Washington DC Metropolitan area in order to facilitate collaboration with myUSCIS Government staff as necessary.
2. USCIS encourages a remote-ready workforce. The Gov't requires in person meetings recurring weekly in Washington DC. with the PM and lead roles. Travel to these recurring meetings will not be covered under the Travel CLIN. As necessary, the contractor shall be available to meet with or remotely collaborate with other USCIS system teams and many of these teams operate in the Washington DC area. Telework and remote employees are acceptable as long as team collaboration, coordination, velocity, and product quality is not negatively impacted. Collaboration will be required between the contractor and Government in order to identify certain roles that can be performed effectively via remote staff.
3. Key meetings with USCIS executives and myUSCIS program leadership primarily occurs at the USCIS offices at 111 Massachusetts Ave & 20 Massachusetts Ave Northwest Washington, DC.

6. Travel (CLIN 0003, 1003, 2003)

1. Travel is required for user research and user testing activities. Travel locations will vary based on the specific user research to be conducted and may include USCIS field offices and service centers, as well as, community based organizations and legal firms. Most travel locations will be within the continental United States, but international travel may also be required. Travel insurance will not be reimbursed by the Government. The Government will not reimburse local travel within a 50-mile radius from the contractor's assigned duty station.
2. Costs associated with long distance travel will be made in accordance with the Federal Travel Regulation and FAR Subpart 31.205-46. All long distance travel shall be pre-approved by the COR.
3. A written request must be sent to both the contracting officer (CO) and the COR and shall be submitted via e-mail at least a week in advance of any anticipated travel in order to allow sufficient time for notification and approval prior to booking travel arrangements.
4. The following information shall be provided in the request:
 - Names of individuals who will be traveling
 - Names of the Government product managers who will provide oversight;

- Inclusive dates and locations of the proposed travel;
- Reason for travel including business justification, goals, activities and expected outcomes; and
- Cost estimate for travel expenses.

All documentation associated with the travel and all receipts shall be submitted with monthly invoices.

7. Government Furnished Property (Reference FAR 52.245-1 Clause)

USCIS will provide contractor staff with Government furnished equipment to include the following:

- MacBook laptop for developers and designers
- Windows laptop for business analysts, PMs, and scrum masters
- Phones for the PM and Leads

Reporting, tracking and proper handling is the responsibility of the contractor.

8. Government Furnished Information & Support

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

9. Documentation

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

9.1 Work Products:

The contractor shall produce work products and deliver them to the IT Program Manager and CSPED product owners. Specific acceptance criteria will be identified with each user story. These are in keeping with Agile methods and principles and vary based on team agreements and structure, scrum vs. Kanban. The contractor is encouraged to suggest alternative Agile methods and sprint durations if those suggested changes are intended to improve team communication, velocity, quality and speed of delivery to production.

9.1.1 Post Implementation Review and a Release Planning Review:

1. In support of TMD, the contractor shall prepare documentation for and attend a combined Post Implementation Review and a Release Planning Review with the CIO and other Government leadership staff from OIT and CPSED. At this meeting, which occurs every six months, the contractor shall provide retrospective details on the previous six month release cycle and shall also outline the roadmap for the upcoming six month release cycle using document templates and guidance from the USCIS Quality Assurance team. These templates outline the capabilities and constraints, system integrations, system design, and pipeline design among other things. The contractor shall for work with the USCIS Federal Program leads to update these documents. Once the CIO approves the release, development continues for another 6 months until the next planning review.
2. The contractor shall produce and deliver documentation that will be the property of USCIS. This documentation shall include technical documentation, system diagrams, code repository information and any and all documents that support transition of support to other contractors.

9.1.2 Work products currently provided given the current 2 week sprint schedule:

| WORK PRODUCT | INTERVAL | DESCRIPTION |
|------------------------------------|-----------------------------------|---|
| Daily Stand Up and Scrum of Scrums | Daily | Discuss daily progress of the sprint, blockers etc. |
| Sprint Review | Every 2 weeks | Demonstrate work that was completed in the sprint; explain work that was not able to be completed. |
| Burn Up Charts | Every 2 weeks at Sprint Review | Explain status of team progress against the scope of work. |
| Sprint Retrospective | Every 2 weeks after Sprint Review | Discuss the sprint, blockers, what went well etc. and use this info to continue to improve performance. |
| Sprint Planning | Every 2 weeks after Sprint Review | Establish sprint goals, plan and prioritize the work to be accomplished in the upcoming sprint including stretch goals. |

| | | |
|--|-----------------------------|--|
| Backlog Grooming | As needed, usually weekly | Groom and prioritize upcoming work and include dependencies. |
| Team Lead Check In | Every 2 weeks, or as needed | Discuss the progress of the overall program, Government's level of satisfaction with the contractor and any issues that need to be addressed. Plan for upcoming meetings or activities, discuss personnel changes. |
| Monthly Status Presentation | Monthly | Accomplishments and upcoming work presented to leadership. |
| Release Planning Review and Post Implementation Review Documentation | Every 6 months | Update documentation Attend the RPR/PIR meeting. |
| Jira Confluence Wiki | Confluence Wiki | Update project documents on the Jira Confluence Wiki on daily basis. |

10. Task Order Deliverables

1. The PM is responsible for formulating and executing and delivering an action plan to correct project issues. (As Needed)
2. The PM shall prepare and deliver a monthly presentation to senior CSPED and OIT leadership with a recap of accomplishments as well as upcoming work. (Monthly)
3. The contractor shall perform user research to discover user needs using methods such as design studios, user interviews, and usability testing. The contractor shall deliver a research plan prior to beginning the sessions, and the contractor shall provide detailed findings in the form of mock up prototypes, presentations after conducting the sessions. (As Needed)
4. The contractor shall plan, organize, facilitate, and collect data from focus group and research/usability testing sessions. The contractor shall provide a moderator's guide that outlines the questions that will be asked. (As Needed)
5. The contractor shall develop a transition plan. (Within 30 days of the Notice to Award)
6. The Contractor must provide a quarterly report that lists the contract name, number, and COR with each Trusted Tester's name, certification level, certification date, certification number, E-mail address, phone number, and supported projects to the COR and USCIS Section 508 Coordinator. This report must also be provided within 10 working days of any change in the Trusted Tester population.

Part IV – Solicitation Provisions/Instructions/Evaluation

Federal Acquisition Regulation (FAR) provisions incorporated by reference

52.217-5 Evaluation of Options (Jul 1990)

52.203-18 Prohibition on Contracting with Entities that Require Certain Internal Confidentiality Agreements or Statements-Representation

5.2225-25 Prohibition on Contracting with Entities Engaging in Certain Activities or Transaction Relating to Iran—Representation and Certifications

Federal Acquisition Regulation (FAR) provisions incorporated in full text

52.209-2 Prohibition On Contracting With Inverted Domestic Corporations-- Representation (Nov 2015)

(a) Definitions. “Inverted domestic corporation” and “subsidiary” have the meaning given in the clause of this contract entitled Prohibition on Contracting with Inverted Domestic Corporations (52.209-10).

(b) Government agencies are not permitted to use appropriated (or otherwise made available) funds for contracts with either an inverted domestic corporation, or a subsidiary of an inverted domestic corporation, unless the exception at 9.108-2(b) applies or the requirement is waived in accordance with the procedures at 9.108-4.

(c) Representation. The offeror represents that—

(1) It [] is, [] is not an inverted domestic corporation; and

(2) It [] is, [] is not a subsidiary of an inverted domestic corporation.

(End of provision)

52.209-11 Representation by Corporations Regarding Delinquent Tax Liability or a Felony Conviction under any Federal Law (Feb 2016)

(a) As required by sections 744 and 745 of Division E of the Consolidated and Further Continuing Appropriations Act, 2015 (Pub. L 113-235), and similar provisions, if contained in subsequent appropriations acts, the Government will not enter into a contract with any corporation that--

(1) Has any unpaid Federal tax liability that has been assessed, for which all judicial and administrative remedies have been exhausted or have lapsed, and that is not being paid in a timely manner pursuant to an agreement with the authority responsible for collecting the tax liability, where the awarding agency is aware of the unpaid tax liability, unless an agency has considered suspension or debarment of the corporation and made a determination that suspension or debarment is not necessary to protect the interests of the Government; or

(2) Was convicted of a felony criminal violation under any Federal law within the preceding 24 months, where the awarding agency is aware of the conviction, unless an agency has considered suspension or debarment of the corporation and made a determination that this action is not necessary to protect the interests of the Government.

(b) The Offeror represents that—

(1) It is is not a corporation that has any unpaid Federal tax liability that has been assessed, for which all judicial and administrative remedies have been exhausted or have lapsed, and that is not being paid in a timely manner pursuant to an agreement with the authority responsible for collecting the tax liability; and

(2) It is is not a corporation that was convicted of a felony criminal violation under a Federal law within the preceding 24 months.

(End of provision)

52.216-1 Type of Contract

(Apr 1984)

The Government contemplates award of a **FIRM FIXED PRICE** contract resulting from this solicitation.

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

3052.209-72 Organizational Conflict of Interest

(Jun 2006)

(a) Determination. The Government has determined that this effort may result in an actual or potential conflict of interest, or may provide one or more offerors with the potential to attain an unfair competitive advantage. The nature of the conflict of interest and the limitation on future contracting for any requirements dealing with Independent Verification and Validation (IV & V).

(b) If any such conflict of interest is found to exist, the Contracting Officer may (1) disqualify the offeror, or (2) determine that it is otherwise in the best interest of the United States to contract with the offeror and include the appropriate provisions to avoid, neutralize, mitigate, or waive such conflict in the contract awarded. After discussion with the offeror, the Contracting Officer may determine that the actual conflict cannot be avoided, neutralized, mitigated or otherwise resolved to the satisfaction of the Government, and the offeror may be found ineligible for award.

(c) Disclosure: The offeror hereby represents, to the best of its knowledge that **(check one):**

___ (1) It is not aware of any facts which create any actual or potential organizational conflicts of interest relating to the award of this contract, or

___ (2) It has included information in its proposal, providing all current information bearing on the existence of any actual or potential organizational conflicts of interest, and has included a mitigation plan in accordance with paragraph (d) of this provision.

(d) Mitigation. If an offeror with a potential or actual conflict of interest or unfair competitive advantage believes the conflict can be avoided, neutralized, or mitigated, the offeror shall submit a mitigation plan to the Government for review. Award of a contract where an actual or potential

conflict of interest exists shall not occur before Government approval of the mitigation plan. If a mitigation plan is approved, the restrictions of this provision do not apply to the extent defined in the mitigation plan.

(e) Other Relevant Information: In addition to the mitigation plan, the Contracting Officer may require further relevant information from the offeror. The Contracting Officer will use all information submitted by the offeror, and any other relevant information known to DHS, to determine whether an award to the offeror may take place, and whether the mitigation plan adequately neutralizes or mitigates the conflict.

(f) Corporation Change. The successful offeror shall inform the Contracting Officer within thirty (30) calendar days of the effective date of any corporate mergers, acquisitions, and/or divestures that may affect this provision.

(g) Flow-down. The contractor shall insert the substance of this clause in each first tier subcontract that exceeds the simplified acquisition threshold.

(End of provision)

Instructions to Offerors

A) POINT OF CONTACT

All questions regarding this solicitation shall be addressed to the Contracting Officer via the Contract Specialist at the following e-mail addresses:

Main: Celina.R.Hemingway@uscis.dhs.gov

Cc: ContractingProposals@uscis.dhs.gov

B) OFFER SUBMITTAL INSTRUCTIONS (*PROPOSALS SHALL INCLUDE PROPRIETARY MARKINGS*)

There will be 4 factors evaluated for this procurement. In determining award, the Government will consider the following factors that are listed in descending order of importance with Factor 1 being most important. When combined, all non-price factors are considerably more important than price.

Factor 1 - Technical Challenge (Phase 2) – (Paperless)

Factor 2 - Design Demonstration (Phase 1) – (Paperless)

Factor 3 – Approach to Staffing (Phase 2) – (Explanation- Limit 5 pages (including cover page, 10 pt font)

Factor 4 – Price (Phase 1 & 2) –Price shall be submitted during Phase 1 (On provided Excel Spread Sheet Attachment #4, along with, Business Volume – no page limit, 10 point font)

The evaluation of proposals shall proceed via a 2 phase process. Phase 1, will be an evaluation of Factor 2 Design Demonstration and Factor 4 Price. A tradeoff analysis will not be conducted during Phase 1. The Government will determine the most highly rated offers, with prices determined to be reasonable in phase 1, who may proceed to participate in Phase 2.

Phase 2 will be an evaluation of Factor 1 Technical Challenge, Factor 3 Approach to Staffing and Factor 4 Price. Proposals are due by date and time shown on page 1, box 18 of SF1447.

Proposals shall be submitted by email to ContractingProposals@uscis.dhs.gov with a copy to the contract specialist Celina.R.Hemingway@uscis.dhs.gov and shall arrive by the date and time set for receipt of offers. The e-mail's subject line shall read: myUSCIS [OFFERING CONTRACTOR NAME].

C) Estimated timeframes are as follows:

- a. Phase 1 evaluations are estimated to be completed by the week of July 9th, 2018.
- b. Invitations to Phase 2 are estimated to be issued the week of July 16th, 2018.
- c. Phase 2 technical demonstrations are anticipated to take place between July 25th, 2018 and August 8th, 2018.

PHASE 1 – Evaluation of Factor 2 Design Demonstration and Factor 4 Price

Factor 2 – Design Demonstration

The Offeror shall submit two (2) examples of design work performed during the past 3 years. For each work example, the Offeror shall submit a publicly accessible URL allowing the Government to view the actual product designed by the Offeror. At least one of the design work examples must have been performed by the prime contractor. The URL for the work example may link to the live site that resulted from the project or a link to a demonstration site that represents the work done on the project. The government will also accept an example of previous design work in the form of a responsive mobile application. The URL provided may be a link to the mobile application in the google play store or iTunes store, and will be evaluated by downloading, running and testing the app on a mobile device. Work samples can be from the private sector or public sector (Government) work, no preference will be given to federal government work. The Government will not accept password protected sites.

The work examples may include sub-webpages. The Government is able to review and include in its evaluation multiple sub-webpages associated with the Offeror's design work examples. For example - An Offeror submits www.nike.com as a work example and the Offeror's video narrative mentions that they also designed features on multiple subpages of Nike's website, such as those associated with the Nike Plus Membership web experience. The government may review those subpages and include them in its evaluation.

Additionally, the Offeror shall submit a video via YouTube that discusses design activities that the Offeror employed on each work example. Specifically, the Offeror's video shall include the following information for each work example:

- 1) What was the problem that your design solved?
- 2) Defend the design decisions made for each URL, and describe how 3 of the 6 key techniques listed below were utilized. The 3 key techniques need not be discussed for

each URL, but a total of 3 must be discussed throughout the video. In the beginning of the video vendors shall clearly identify the 3 key techniques that are submitted for evaluation.

- User Research
- Interaction Design
- Usability Testing
- Visual Design
- Content Strategy
- Information Architecture

The Offeror's video submission shall be no longer than 5 minutes and shall cover both of the Offeror's work examples combined.

Videos must be posted and submitted to USCIS as an "unlisted" or "private" Youtube.com link. myUSCIS has an established YouTube account under the email address of celina.r.hemingway@uscis.dhs.gov. If a "private" Youtube.com link is provided, the Offeror shall share the "private" link with myUSCIS' account and USCIS Contracting Office using the following e-mail(s):

Contract Specialist: Celina.R.Hemingway@uscis.dhs.gov

Note: Regarding the URL to the YouTube video, it is important that the Offeror does not send in a truncated URL because those truncated YouTube URLs are blocked on DHS's network. Example - <https://www.youtube.com/watch?v=6ZfuNTqbHE8> is acceptable but <https://youtu.be/6ZfuNTqbHE8> is not acceptable. The URLs shall be provided in the written response email to the email addresses listed in the RFP.

Prior to submission, Offerors should check the URLs to be sure they are not broken and that content is accessible. **If the content cannot be accessed by the government, the Offeror's proposal submission will be determined to be non-compliant and will be rejected.**

Factor 4 – Price

- The business volume shall provide pricing in the excel spreadsheet provided (see attachment 4 sample staffing mix) to facilitate the Government's evaluation of the total fixed price to include all optional CLINS for each period of performance.
- The business volume has no page limit and shall include:
 - A cover letter formalizing the quote and include the Offeror's point of contact information, Data Universal Numbering System (DUNS) number, and EAGLE II Contract Number.
 - Detailed pricing breakdown, which includes the base period and all options, clearly showing the connection from the contractor's proposed rates and how

those rates compare to its parent EAGLE II contract to this offer. Pricing shall be no greater than Offerors' EAGLE II approved rates.

- If the offer includes discounts from the parent contract's pricing rates, those discounts should be shown and explained in the business volume so the contracting officer can understand the basis for the discount.
- The Government estimates this requirement may range in price from \$75M to \$95M, which includes all option periods and all optional CLINS. The government has provided the range to facilitate the development of the proposals. A proposal outside of those ranges can still be determined to be acceptable as long as the rates proposed are less than or equal to established EAGLE II rates.
- All information responses to solicitation provisions.
- An unambiguous statement that the Offeror agrees to all clauses, terms, or conditions shown in the solicitation.
- Populated pricing information for each CLIN. Offerors are encouraged to manipulate the sample staffing mix attachment #4 to provide the pricing. This spreadsheet includes the labor categories proposed and number of FTEs, therefore, contractors can simply insert the proposed pricing for each CLIN.
- Offerors shall provide a price for all CLINs, excluding Travel, as the Government has provided a not to exceed amount for travel.
- This is a fixed price task order; however, Offerors are required to provide the proposed EAGLE II rates and any discounts (as a percentage).
- Price will be evaluated in both phases. Pricing submitted in Phase 1 shall include all of the written information required. The pricing submitted in Phase 1 will be used in both phases and shall not need to be provided a second time for Phase 2.

PHASE 2 – Evaluation of Factor 1 Technical Challenge, Factor 3 Approach to Staffing and Factor 4 Price

The government will notify offerors invited to Phase 2 seven (7) calendar days prior to their scheduled challenge date. Along with the invitation for phase 2 the Government will supply details and needed information for the technical challenge.

Offerors are not required to start from scratch on the day of the Technical Challenge. The government plans to distribute details about the Technical Challenge after Phase 1, such as a product vision. Additional information is expected to be provided to Offerors on the day of their Technical Challenge. That information is expected to be related to user needs, business goals, and the API.

Factor 1 - Technical Challenge

Three (3) calendar days prior to their technical challenge date, Offerors shall submit:

Factor 1 – Technical Challenge Items (via e-mail using submission guidance above)

- List of technical stack and tools that the Offeror intends to utilize at the technical challenge. Use of tools is at the discretion of the vendor during the technical challenge. The contractor must bring the tools necessary to complete the challenge.
- List of technical challenge attendees and their titles
- Diagram and description of the CI/CD pipeline that the Offeror anticipates using, limited to 1 page.
- Instructions on how to access the Offeror’s repositories and tools that will be used during the technical challenge

Factor 3 – Approach to Staffing Items (via e-mail using the guidance above)

- The populated sample staffing attachment #4 with the proposed FTEs
- Approach to Staffing context and rational explanation, PDF document limited to 5 pages, including cover page, with 10 point font.

Factor 4 – Price

- Price submitted during Phase 1 will be used for Phase 2 – Do not resubmit for Phase 2

The Offeror will participate in a one-day technical challenge that will be used to evaluate the Offeror’s ability to perform the scope of support required for the myUSCIS task order.

Companies and individuals are precluded from showing up at multiple technical demonstrations. This is necessary to ensure the integrity of the technical demo evaluation.

All technical challenges will be videotaped to be retained by the government for the contract file. All items produced by the offerors during the challenge including, but not limited to documents, notes, and whiteboard artifacts will be collected at the conclusion of the challenge. Any technical challenge resulting work products shall not be used publicly by the offeror for its own purposes following award.

There will be no government product owner or user representative for direct interaction with the challenge team during the challenge to clarify user stories, priorities, discuss trade-off decisions between user needs, business goals, and technical feasibility. There will be an API technical resource in the room that will be available for clarification needs during the challenge.

During this myUSCIS technical challenge, the Offeror shall leverage Digital Service Playbook concepts (www.playbook.cio.gov) to design, develop, and continuously deploy a Minimum Viable Product (MVP). Following the deployment of the MVP, the Offeror shall present a demonstration of their MVP and discuss the decisions made in producing the MVP. The presentation format of the Offeror’s MVP demonstration is at the Offeror’s discretion, including the extent to which an Offeror chooses to use slides or other presentation tools and techniques.

The estimated schedule for the technical challenge day is as follows. This schedule may change day to day, however each vendor will be given the 5 hours for technical challenge, and 30 minutes for the demonstration:

8:00 am - Offeror Arrival to Technical Challenge Room
8:15 am - Introductions & Logistics
8:30 am - Offeror Begin Setup
9:00 am - Technical Challenge Begins
2:00 pm - Tech Challenge Ends & Offeror's Demonstration Preparation Begins
3:00 pm - MVP Demonstration Begins
3:30 pm - MVP Demonstration Ends
3:45 pm - Government Clarification Questions Begins
5:00 pm - Offeror Departs

The exact schedule for the technical challenge will be provided to Offerors when they receive their technical challenge date appointment. The technical challenge exercise will take place at a Government facility in the Washington DC metro area. The exact location of the technical challenge exercise will be provided when the Government provides the Offeror with its technical challenge appointment date. The contracting officer (CO) will determine the order in which Offerors are scheduled. Requests to reschedule will be at the discretion of the CO.

The technical challenge allows the vendor 5 hours to design, develop, and deploy their MVP. Offerors will be allowed to bring up to a maximum of 10 individuals to perform the technical challenge. The team attending the technical challenge is expected to be representative of what the Offeror would provide the Government after contract award. The individuals attending the technical challenge are not expected to be staffed on the myUSCIS task order and key personnel are not required to participate in the technical challenge. Additionally, the Offeror is allowed to bring a Corporate Representative who will be able to observe their team's performance and will not perform any technical challenge activities including, but not limited to, design, developing, deploying, and demonstrating the MVP.

It is up to the Offeror to budget time for food and drinks during the day. Offerors are allowed to bring food and drinks with them to the Technical Challenge. Additionally, the government will allow non-challenge day participants to deliver food and drinks to the facility. Those individuals cannot enter the room where the Technical Challenge is occurring. The vendor must provide their own equipment for the technical challenge, including but not limited to, internet access and any supplies needed (sticky notes, computer, food, drinks, etc.). The vendor shall arrive early enough to check into the facility and validate that they are able to begin the demonstration on time.

For the technical challenge, the Offeror shall design, develop, and deploy an application to a cloud environment. The details and needed information for the technical challenge will be supplied along with the invitation to the vendor for Phase 2. The government plans to distribute details about the Technical Challenge after Phase 1, such as a product vision. Additional information is expected to be provided to Offerors on the day of their Technical Challenge. This content will primarily be related to user needs and business goals and is expected to form the

foundation for the Offeror's design activities and related decision-making during the technical challenge. This content will be in the form of materials such as a product vision, user stories and the API.

The Offeror shall use a modern technical development stack, tools, and CI/CD pipeline to design, develop, and deploy the application. The Offeror shall provide the Government real-time access to any and all systems utilized by the vendors for the challenge including but not limited to artifacts, code repositories and tools used. The Government shall be able to access e-artifacts, code repositories and tools from current Government furnished equipment rather than vendor supplied equipment. The Offeror shall provide the Government with access to the tools & repositories up to the date of task order award.

During the technical challenge, the Offeror shall integrate their MVP with a Government-provided API. The Government will provide the Offeror with access information and credentials. The deployed MVP will need to interact with the API, using the supplied credentials.

The Offeror's MVP demonstration will allow the Government to experience the MVP produced by the Offeror and to hear the rationale behind the Offeror's decision-making in designing, developing, and deploying the MVP. Offerors are strongly discouraged from discussing content unrelated to the technical challenge, such as discussing corporate capabilities.

Factor 3 - Approach to Staffing

Offerors shall submit their proposed staffing mix using the sample staffing attachment #4, including base and all option periods and an explanation of the context and rationale of the mix, in a PDF document limited to 5 pages, including cover page, using 10 point font.

The maximum number of FTEs, to include all optional CLINs, to be staffed on this task order will be 73 FTEs for the base and 83 FTEs for each of the option years.

The Government provided a sample staffing mix, not to be construed as the best technical approach, but one to guide the Offerors in developing their staffing mix. Offeror's are not encouraged to copy sample staffing mix, but should propose their own innovative staffing composition. When proposing their staffing mix, Offerors shall adjust the spreadsheet as necessary to fit their proposal, while maintaining the CLIN structure organization, as pricing shall be provided that aligns to the CLIN structure. See pricing instructions for further details on proposal pricing. Staffing Mix and pricing are provided on attachment #4 during phase 1 (only submitted once). Factor 3 - Approach to Staffing additional documentation (5 page PDF supporting rational) shall be submitted in phase 2.

For the purposes of the sample staffing mix a full time equivalent in Attachment #4 assumes 1,920 hours annum. Contractors SHALL NOT provide the assumption for hours for an FTE, the Government is only providing it to further support the contractors understanding of the sample staffing levels. Contractors SHALL NOT propose hours, rather propose FTE team composition. If contractors are proposing less than a full time person (i.e. less than 1,920 hours in Attach 1)

they may propose to the 10th (for example: .5 FTE, .3 FTE). The Government does not need to know or understand the hour's annum buildup for the FTE's proposed.

If a contractor's DCAA-approved forward pricing rate agreement (FPRA) and DHS EAGLE II rate schedule is based on something other than 1,920 hours per annum for a full time equivalent number of hours, it is acceptable to use the contractor's FPRA hours per annum to generate cost per FTE and detail this in the business volume.

Factor 4 – Price

(Price submitted during Phase 1 will be used for Phase 2 – Do not resubmit for Phase 2)

Evaluation and Selection

1. BASIS FOR AWARD

The Government intends to award one task order from this solicitation. Determination of best value will be made by using a tradeoff process. The Government intends to make a task order award without discussions; however, the Government reserves the right to hold discussions. In determining award, the Government will consider the following factors that are listed in descending order of importance with Factor 1 being most important. When combined, all non-price factors are considerably more important than price.

Factor 1 - Technical Challenge (Phase 2) – (Paperless)

Factor 2 - Design Demonstration (Phase 1) – (Paperless)

Factor 3 – Approach to Staffing (Phase 2) – (Explanation- Limit 5 pages (including cover page, 10 pt font)

Factor 4 – Price (Phase 1 & 2) –Price shall be submitted during Phase 1 (On provided Excel Spread Sheet, along with, Business Volume – no page limit, 10 point font)

Phase 1, evaluation of Factor 2 – Design Demonstration and Factor 4 Price, is a mandatory firm down-select. The Government will assess each Offeror's design capability in order to identify the most highly-rated Offerors. Phase 1 is a most highly rated offer evaluation. Trade-off will **not** be applied at Phase 1. The most highly rated offers, with prices determined to be reasonable in phase 1, may proceed to participate in Phase 2 -Evaluation of Factors 1, 3 and 4. Trade-off will apply at Phase 2. The Government will include as part of the trade off at the final phase (phase 2), the results from Phase 1. The Factor 4 price submitted during Phase 1 will be the final price used for the trade-off decision.

It is anticipated that the same evaluation team members will evaluate all Offerors.

PHASE 1 – Evaluation of Factors 2 and 4

Factor 2 - Design Demonstration: This factor will be evaluated as Outstanding, Good, Acceptable, or Unacceptable. The Government will evaluate the degree to which the Offeror’s work examples and video narrative effectively demonstrates how the design decisions solve the design problem associated with each of two the work sample submissions. Each work sample is equally rated. The Government’s evaluation may include multiple sub-webpages associated with the Offeror’s design work examples. Contractors are encouraged not to include jargon in the video.

The Government’s design demonstration evaluation will evaluate the Offeror’s design decisions, utilizing 3 of the following key areas, which are weighted equally:

1. User Research
2. Interaction Design
3. Usability Testing
4. Visual Design
5. Content Strategy
6. Information Architecture

The government is going to evaluate the Offerors use of 3 design techniques. The content of the video is at the discretion of the Offeror, but the government will only be evaluating 3 techniques. If those 3 techniques are not clearly identified in the video, then the government will evaluate 3 techniques that they observe throughout the video.

The government will base its evaluation on the content of the video and not on quality of the filming methods, graphics, or equipment used. The Government’s evaluation of the design demonstration video will stop at 5 minutes; any content beyond 5 minutes will not be evaluated. The Government will evaluate if the examples of design work were performed during the past 3 years. The Government will also evaluate how well the video identified the problem, and how well the video explained how the problem was solved. The Government will also evaluate the use or over use of jargon in the video. Per Dictionary.com: “Jargon - Language that is characterized by uncommon or pretentious vocabulary and convoluted syntax and is often vague in meaning.”

Factor 4 – Price

The Government will evaluate the total fixed price to include all optional CLINS (for example CLINs 0001 to 0006 in the first period of performance) and will do the same for each of the option periods.

The Government will evaluate that the contractor’s proposed EAGLE II rates comply with the EAGLE II contract. Proposals exceeding those rates will not be considered for award.

The Government will evaluate discounts proposed (**as a percentage**) and if necessary perform price realism on rates that are significantly discounted. The determination of significant is at the discretion of the contracting officer.

PHASE 2 – Evaluation of Factors 1, 3 and 4

Factor 1 - Technical Challenge

The Offeror's performance during the challenge will be evaluated as Outstanding, Good, Acceptable, or Unacceptable based on the following criteria and all are equally important:

1. The extent to which the Offeror effectively makes tradeoff decisions between user needs, business goals, and technical feasibility.
2. The degree to which the Offeror's coding practices and related decisions result in a maintainable codebase.
3. The degree to which the Offeror's MVP is effectively integrated with the Government-provided API.
4. The degree to which the Offeror effectively implements a CI/CD pipeline for their MVP, including their effective use of automated testing and automated code quality checks.

Factor 3 – Approach to Staffing

The approach to staffing will be evaluated as Outstanding, Good Acceptable, or Unacceptable. The Government will evaluate labor mix proposed (FTEs NOT hours), as the level of effort has been established, and supporting rationale for how the contractor understands the SOW and will successfully perform the task order requirements.

Factor 4 – Price

The Government will evaluate the total fixed price to include all optional CLINS (for example CLINs 0001 to 0006 in the first period of performance) and will do the same for each of the option periods.

The Government will evaluate that the contractor's proposed EAGLE II rates comply with the EAGLE II contract. Proposals exceeding those rates will not be considered for award.

The Government will evaluate discounts proposed (**as a percentage**) and if necessary perform price realism on rates that are significantly discounted. The determination of significant is at the discretion of the contracting officer.

| <u>Ratings (Table A)</u> <u>For Factors 1, 2, and 3</u> | |
|---|---|
| *When referring to proposal this includes the offerors design demonstration and technical challenge * | |
| Rating | Definitions |
| Outstanding | Proposal demonstrates a superior understanding of the requirements. Their approach significantly exceeds the design demonstration/technical challenge requirements. Proposal has multiple strengths that benefit the Government. Proposal has no significant weaknesses, or deficiencies. Risk of unsuccessful performance is very low. |
| Good | Proposal demonstrates a good understanding of the requirements and an approach that exceeds the design demonstration/technical challenge requirements. Proposal has strengths that benefit the Government. The proposal may contain weaknesses, but cannot contain any deficiencies. Risk of unsuccessful performance is low. |
| Acceptable | Proposal demonstrates an understanding of the requirement and an approach that meets the design demonstration/technical challenge requirements. Proposal may contain weaknesses or may have no strengths, but risk of unsuccessful performance is low to moderate. The proposal may not contain any deficiencies. |
| Unacceptable | Proposal does not demonstrate an understanding of the requirements and the approach does not meet the design demonstration/technical challenge requirements. Proposal presents an unacceptable solution. Proposal contains at least one or more deficiencies and or multiple weaknesses or significant weaknesses and appreciably increases risk of unsuccessful performance. |

Key Definitions

Strength: An element of a proposal which exceeds a requirement of the solicitation in a beneficial way to the Government.

Weakness: A flaw in a proposal that increases the chance of unsuccessful performance.

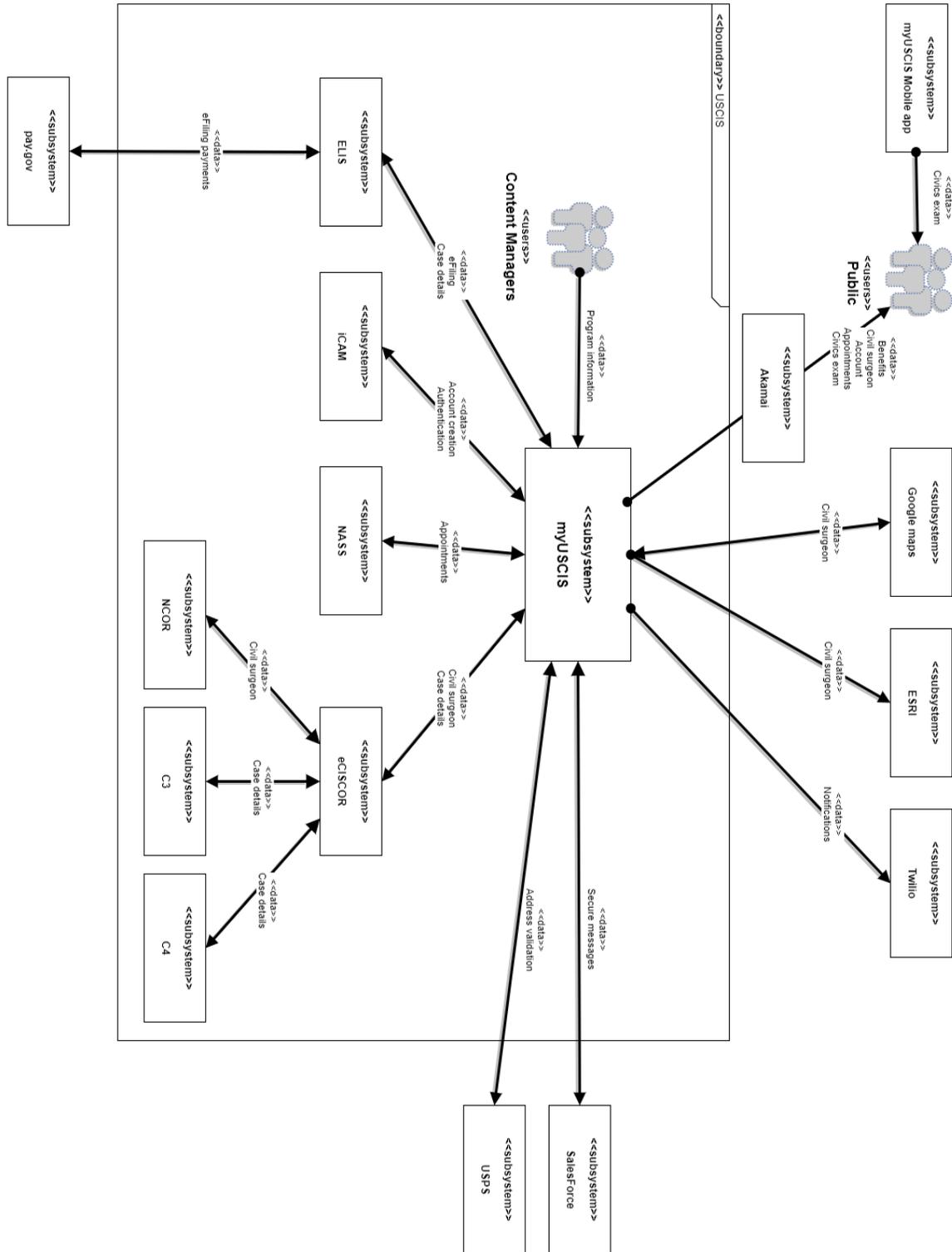
Significant Weakness: A flaw in a proposal that appreciably increases the risk of unsuccessful contract performance.

Deficiency: A material failure of an offer or quotation to meet a Government requirement or a combination of significant weaknesses in an offer or quotation that increases the risk of unsuccessful contract performance to an unacceptable level.

myUSCIS SOW Attachment #1 myUSCIS System Integrations – Diagram

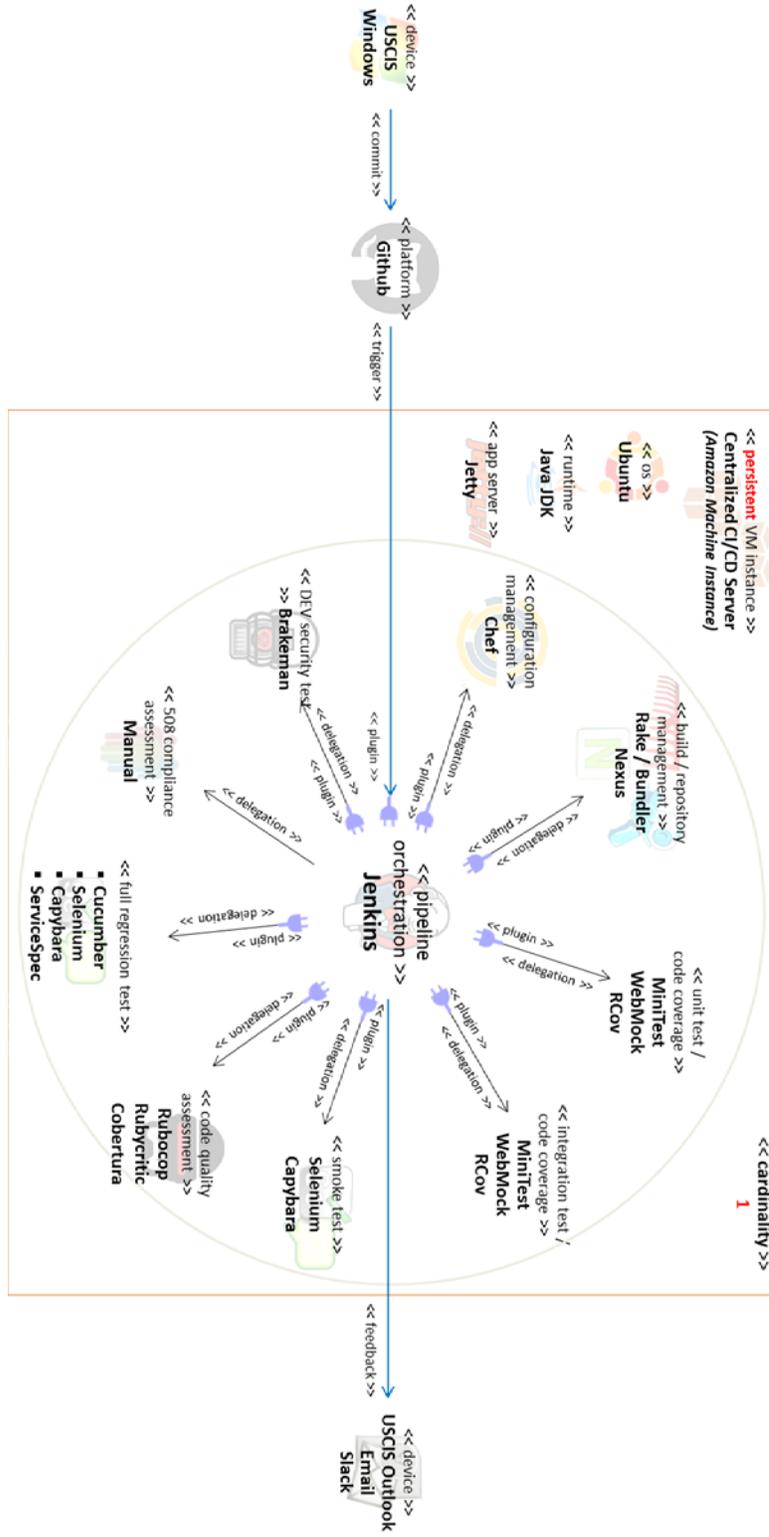
SOW Attachment # 1:

The following diagram provides additional detail on the current systems that are integrated with myUSCIS (this is subject to change)



SOW Attachment #2: Current Pipeline - Diagram

The current pipeline diagram is included below. The tools used in the pipeline are subject to change.



SOW Attachment #3: The current technical stack & tools

Current Technical Stack & Tools

The myUSCIS technical stack and tools changes rapidly due to the Agile nature of the program. It is expected that this will continue to evolve and the Government will expect the Contractor to continue to research and suggest tools that will improve and evolve the technology stack while reducing costs. The current stack consists of predominately open source tools. The myUSCIS application resides in the AWS Commercial Cloud and also uses several of the AWS cloud services. The CI/CD pipelines were custom built using industry best practices, AWS services and open source tools. The DevOps documentation resides in GHE. myUSCIS is written primarily in Ruby on Rails with some React and Java.

The current set of tools is listed in Table 1 below. This is not an exhaustive list and is subject to change.

Table 1 – Technical Stack and Tools for my.USCIS.gov

| | |
|------------------------------------|--|
| Design Tools | Mural Sketch InVision Adobe Creative Cloud |
| Operating System | Linux Ubuntu |
| Programming Languages | Ruby on Rails React React Native Python Java R TensorFlow numPy |
| Pipeline Orchestration | Jenkins |
| Databases/ Storage Services | AWS RDS PostgreSQL S3 Neo4J |
| Data Analytics Platform | DataBricks |
| Akamai | Content Delivery Network |
| AWS tools | Elastic search CloudFormation Elastic GPU |
| Source Code Version Control | GitHub Enterprise (GHE) |
| Configuration Management | Chef |
| Testing Tools | Selenium Jmeter MiniTest WebMock Enzyme React-Mock Cucumber Capybara ServiceSpec Ava FireEyes WorldSpace Brakeman CarWash |
| Build Tools | Rake Bundler React-Native |

myUSCIS SOW Attachment #3
Current Technical Stack & Tools

| | |
|------------------------------------|---|
| | Docker Packer Python |
| Code Coverage for Unit Test | RCov Istanbul PyTest Coverage |
| Code Quality Assessment | RuboCop rubycritic Cobertura Common JavaScript PyLint |
| Monitoring Tools | New relic Google Analytics Cloudwatch Akamai SPIDER/Splunk Jenkins |

Attachment # 4
myUSCIS Government Sample Staffing Mix and CLIN Structure

| | myUSCIS Labor Category - GOVERNMENT SAMPLE | myUSCIS Labor Category - CONTRACTOR PROPOSED | myUSCIS Labor Rate - CONTRACTOR RATE PROPOSED | Eagle II FC1 Unrestricted Contractor Site Labor Category | CLIN# | GOVERNMENT SAMPLE FTEs | CONTRACTOR PROPOSED FTEs | TOTAL PROPOSED PRICE |
|--|--|---|--|--|-------------|---------------------------|-----------------------------|----------------------------|
| | Program Management Transition In | Firm Fixed Price (4 MO) | Firm Fixed Price | | 0006 | | | |
| | Program Manager | | | | | 1 | | |
| | Senior Project Manager | | | | | 1 | | |
| | Project Manager | | | | | 1 | | |
| | | | TOTAL PM TRANSITION | | | 3 | | |
| | Technical Support and Agile Teams Transition In | Firm Fixed Price (4 MO) | Firm Fixed Price | | 0007 | | | |
| | Technical Lead | | | | | 1 | | |
| | DevOps Lead | | | | | 1 | | |
| | Designer Lead | | | | | 1 | | |
| | Data Scientists | | | | | 2 | | |
| | Data Engineers | | | | | 2 | | |
| | Ethnographer | | | | | 1 | | |
| | Business Process Analyst | | | | | 2 | | |
| | 4 Agile Teams: | | | | | | | |
| | DevOps Engineer / Senior | | | | | 4 | | |
| | Scrum Master/Kanban Master | | | | | 4 | | |
| | Developer | | | | | 20 | | |
| | Designer | | | | | 12 | | |
| | | | TOTAL TECHNICAL TRANSITION | | | 50 | | |
| | CLIN 0006 AND 0007 FALL OFF IN THE OPTION PERIODS | | | | | | | |

Attachment # 4
myUSCIS Government Sample Staffing Mix and CLIN Structure

| | myUSCIS Labor Category - GOVERNMENT SAMPLE | myUSCIS Labor Category - CONTRACTOR PROPOSED | myUSCIS Labor Rate - CONTRACTOR RATE PROPOSED | Eagle II FC1 Unrestricted Contractor Site Labor Category | CLIN# | GOVERNMENT SAMPLE FTEs | CONTRACTOR PROPOSED FTEs | TOTAL PROPOSED PRICE |
|--|---|---|--|---|-------|---------------------------|--------------------------------|----------------------------|
| | Program Management | Firm Fixed Price (5 MO) | Firm Fixed Price (5 MO) | | 0001 | | | |
| | Program Manager | | | | | 1 | | |
| | Senior Project Manager | | | | | 1 | | |
| | Project Manager | | | | | 1 | | |
| | | | TOTAL PROGRAM MANAGEMENT | | | 3 | | |
| | Technical Support and Agile Teams | Firm Fixed Price (5 MO) | Firm Fixed Price (5 MO) | | 0002 | | | |
| | Technical Lead | | | | | 1 | | |
| | DevOps Lead | | | | | 1 | | |
| | Designer Lead | | | | | 1 | | |
| | Data Scientists | | | | | 2 | | |
| | Data Engineers | | | | | 2 | | |
| | Ethnographer | | | | | 1 | | |
| | Business Process Analyst | | | | | 2 | | |
| | 4 Agile Teams: | | | | | | | |
| | DevOps Engineer / Senior | | | | | 4 | | |
| | Scrum Master/Kanban Master | | | | | 4 | | |
| | Developer | | | | | 20 | | |
| | Designer | | | | | 12 | | |
| | | | TOTAL TECHNICAL | | | 50 | | |
| | ODC CLIN: Travel | | Reimbursable at Cost | | 0003 | | | \$25,000 |
| | OPTIONAL CLINS (5 MO) | | | | | | | |
| | 1 Optional Agile Team | | Firm Fixed Price | | 0004 | | | |
| | DevOps Engineer / Senior | | | | | 1 | | |
| | Scrum Master/Kanban Master | | | | | 1 | | |
| | Developer | | | | | 5 | | |
| | Designer | | | | | 3 | | |
| | | | TOTAL OPTIONAL TEAM | | | 10 | | |
| | OPTIONAL CLINS (5 MO) | | | | | | | |
| | 1 Optional Agile Team | | Firm Fixed Price | | 0005 | | | |
| | DevOps Engineer / Senior | | | | | 1 | | |
| | Scrum Master/Kanban Master | | | | | 1 | | |
| | Developer | | | | | 5 | | |
| | Designer | | | | | 3 | | |
| | | | TOTAL OPTIONAL TEAM | | | 10 | | |

Attachment # 4
myUSCIS Government Sample Staffing Mix and CLIN Structure

| myUSCIS Labor Category - GOVERNMENT SAMPLE | myUSCIS Labor Category - CONTRACTOR PROPOSED | myUSCIS Labor Rate - CONTRACTOR RATE PROPOSED | Eagle II FC1 Unrestricted Contractor Site Labor Category | CLIN# | GOVERNMENT SAMPLE FTEs | CONTRACTOR PROPOSED FTEs | TOTAL PROPOSED PRICE |
|---|---|--|---|-------------|---------------------------|--------------------------------|----------------------------|
| Program Management | Firm Fixed Price (12 MO) | Firm Fixed Price | | 1001 | | | |
| Program Manager | | | | | 1 | | |
| Senior Project Manager | | | | | 1 | | |
| Project Manager | | | | | 1 | | |
| | | TOTAL PROGRAM MANAGEMENT | | | | | |
| Technical Support and Agile Teams | Firm Fixed Price (12 MO) | Firm Fixed Price | | 1002 | | | |
| Technical Lead | | | | | 1 | | |
| DevOps Lead | | | | | 1 | | |
| Designer Lead | | | | | 1 | | |
| Data Scientists | | | | | 2 | | |
| Data Engineers | | | | | 2 | | |
| Ethnographer | | | | | 1 | | |
| Business Process Analyst | | | | | 2 | | |
| 5 Agile Teams: | | | | | | | |
| DevOps Engineer / Senior | | | | | 5 | | |
| Scrum Master/Kanban Master | | | | | 5 | | |
| Developer | | | | | 25 | | |
| Designer | | | | | 15 | | |
| | | TOTAL TECHNICAL | | | 63 | | |
| ODC CLIN: Travel | | Reimbursable at Cost | | 1003 | | | \$60,000 |
| OPTIONAL CLINS (12 MO) | | | | | | | |
| 1 Optional Agile Team | | Firm Fixed Price | | 1004 | | | |
| DevOps Engineer / Senior | | | | | 1 | | |
| Scrum Master/Kanban Master | | | | | 1 | | |
| Developer | | | | | 5 | | |
| Designer | | | | | 3 | | |
| | | TOTAL OPTIONAL TEAM | | | 10 | | |
| OPTIONAL CLINS (12 MO) | | | | | | | |
| 1 Optional Agile Team | | Firm Fixed Price | | 1005 | | | |
| DevOps Engineer / Senior | | | | | 1 | | |
| Scrum Master/Kanban Master | | | | | 1 | | |
| Developer | | | | | 5 | | |
| Designer | | | | | 3 | | |
| | | TOTAL OPTIONAL TEAM | | | 10 | | |

Attachment # 4
myUSCIS Government Sample Staffing Mix and CLIN Structure

| myUSCIS Labor Category - GOVERNMENT SAMPLE | myUSCIS Labor Category - CONTRACTOR PROPOSED | myUSCIS Labor Rate - CONTRACTOR RATE PROPOSED | Eagle II FC1 Unrestricted Contractor Site Labor Category | CLIN# | GOVERNMENT SAMPLE FTEs | CONTRACTOR PROPOSED FTEs | TOTAL PROPOSED PRICE |
|---|---|--|---|-------------|---------------------------|--------------------------------|----------------------------|
| Program Management | Firm Fixed Price (12 MO) | Firm Fixed Price | | 2001 | | | |
| Program Manager | | | | | 1 | | |
| Senior Project Manager | | | | | 1 | | |
| Project Manager | | | | | 1 | | |
| | | TOTAL PROGRAM MANAGEMENT | | | | | |
| Technical Support and Agile Teams | Firm Fixed Price (12 MO) | Firm Fixed Price | | 2002 | | | |
| Technical Lead | | | | | 1 | | |
| DevOps Lead | | | | | 1 | | |
| Designer Lead | | | | | 1 | | |
| Data Scientists | | | | | 2 | | |
| Data Engineers | | | | | 2 | | |
| Ethnographer | | | | | 1 | | |
| Business Process Analyst | | | | | 2 | | |
| 5 Agile Teams: | | | | | | | |
| DevOps Engineer / Senior | | | | | 5 | | |
| Scrum Master/Kanban Master | | | | | 5 | | |
| Developer | | | | | 25 | | |
| Designer | | | | | 15 | | |
| | | TOTAL LABOR | | | 63 | | |
| ODC CLIN: Travel | | Reimbursable at Cost | | 2003 | | | \$60,000 |
| OPTIONAL CLINS (12 MO) | | | | | | | |
| 1 Optional Agile Team | | Firm Fixed Price | | 2004 | | | |
| DevOps Engineer / Senior | | | | | 1 | | |
| Scrum Master/Kanban Master | | | | | 1 | | |
| Developer | | | | | 5 | | |
| Designer | | | | | 3 | | |
| | | TOTAL OPTIONAL TEAM | | | 10 | | |
| OPTIONAL CLINS (12 MO) | | | | | | | |
| 1 Optional Agile Team | | Firm Fixed Price | | 2005 | | | |
| DevOps Engineer / Senior | | | | | 1 | | |
| Scrum Master/Kanban Master | | | | | 1 | | |
| Developer | | | | | 5 | | |
| Designer | | | | | 3 | | |
| | | TOTAL OPTIONAL TEAM | | | 10 | | |

| Question # | Reference SOW/ Solicitation Section # | Question | Response | Update to RFP | YES/NO |
|------------|--|--|--|--|--------|
| 1 | Page 45 / Data Science, "Support the Overall eProcessing initiative" | Has USCIS determined a timeline for the addition of new USCIS Forms based on the eProcessing initiative? For example, how many forms may be added concurrently and will the development team be responsible for delivering those forms? | We do not know at this time. This is why there are optional CLINs for additional teams | No | |
| 2 | p. 47 / Section 5. Place of Performance | Would the government consider allowing leads to participate in the recurring weekly meetings with USCIS staff remotely? Alternately, would the government consider allowing bi-weekly or monthly in-person participation versus weekly with "off week" participation being remote? | The requirement remains as written. | No | |
| 3 | p. 57 / Phase 2, Factor 1 & 3 | The requirement for the written elements for Factor 3 are required to be two pages long using 10 point font. The description of the CI/CD Pipeline for Factor 1 (Technical Challenge Items) is limited to one page without a stated font requirement. Can offerors assume that we are to use 10 point font for all written submissions for this procurement - Business Volume, Factor 1, Factor 3? | The Vendor assumption is correct. | YES: Update Factor descriptions on pages 54/60 and approach to staffing instructions page 59. | |
| 4 | Page 55, Factor 2 – Design Demonstration | In the instructions for the design demonstration the Government states that "3 key techniques need not be discussed for each URL, but a total of 3 must be discussed throughout the video." Will the Government confirm if Offerors can choose to discuss more than 3 key techniques as long as these are discussed within the timeframe allotted? | The government is going to evaluate the Offerors use of 3 design techniques. The content of the video is at the discretion of the Offeror, but the government will only be evaluating 3 techniques. The government highly recommends that Offeror makes it very clear which 3 techniques that the Offeror is focusing on in their video. If those 3 techniques are not clearly identified in the video, then the government will evaluate 3 techniques that they observe throughout the video. | YES: Updated the Factor 2 - Design Demonstration evaluation paragraph 3 page 61 to include "The government is going to evaluate the Offerors use of 3 design techniques. The content of the video is at the discretion of the Offeror, but the government will only be evaluating 3 techniques. The government highly recommends that Offeror makes it very clear which 3 techniques that the Offeror is focusing on in their video. If those 3 techniques are not clearly identified in the video, then the government will evaluate 3 techniques that they observe throughout the video." Additionally, the RFP Factor 2 - Design Deomnstration instructions, page 55, are updated to include "In The beginning of the video vendors shall clearly identify the 3 key techniques that are submitted for evaluation." | |
| 5 | Instructions to Offerors for Factor 2 – Design Demonstration, on page 55 | The Instructions to Offerors for Factor 2 – Design Demonstration, on page 55 of the solicitation indicate that the offeror must submit examples of design work via a publicly accessible URL. The instructions refer to evaluation of web pages on live or demonstration web sites, but do not explicitly forbid examples of previous work in another form. Since myUSCIS includes a mobile responsive web application, and since mobile application development/support is in the scope described by the Statement of Work, would the government accept an example of previous design work in the form of a responsive mobile application? Provided that it demonstrates the techniques identified for evaluation in the solicitation, can a URL be submitted that provides a link to a responsive mobile app in the Google Play Store or iTunes Store (rather than a traditional web site), that would then be evaluated by downloading, running and testing the app on a mobile device such as a tablet (rather than through web browser)? | The goveremnt will accept an example of previous design work in the form of a responsive mobile application. Additionally, the URL provided may be a link to the mobila app in the google play store or ituens store, and will be evaluated by downloading, running and testing the app on a mobile device. | YES: Updated the Factor 2 - Design Demonstration instruction section, paragraph 1, page 55 to read "The URL for the work example may link to the live site that resulted from the project or a link to a demonstration site that represents the work done on the project. The government will also accept an example of previous design work in the form of a responsive mobile application. The URL provided may be a link to the mobile application in the google play store or iTunes store, and will be evaluated by downloading, running and testing the app on a mobile device." | |
| 6 | Instructions to Offerors on page 54 | May offerors add a cover page to the Approach to Staffing document without counting the cover page against the two-page length limit, to allow for inclusion of administrative information (e.g., company name, point of contact information, etc.) while still allowing two full pages for explanation of the staffing approach? | The government has updated the page limit to be 5 pages, including the cover page, using 10 point font. | YES: Updated Factor descriptions on pages 54/60 and approach to staffing instructions page 59. | |
| 7 | Key Personnel clause on Page 9 | Page 9 of the RFP indicates that the Program Manger considered to be Key Personnel. Could the government clarify expectations for how Offerors are to include proposed Key Personnel in their offers? The instructions for the Approach to Staffing document ask for information on staffing mix and explanation of rationale but do not ask for information on Key Personnel, and personnel qualifications do not appear to be part of the evaluation for Factor 3. Are Offerors expected to include information (experience and qualifications) about the Program Manager, or is this not relevant for evaluation of Offers and is instead something to be designated later upon award? | Key Personnel is not being evaluated and as such, "personnel qualifications" documents are not to be submitted. The requirements for key personnel will be addressed at award and any key personnel introduced at the kick-off shall meet the minimum requirements of the contract or new personnel will need to be indentified by the contractor. | NO | |
| 8 | Section 2 (Tasks), Subsection "Design," page 42 | The government states that the contractor shall work with USCIS to determine usability testing session locations and to recruit users. If this will be the contractor's responsibility, can the government estimate how many usability testing sessions will be conducted and with how many users for each? There are often costs associated with testing facility rental and incentives needed to effective recruit users. Will the government cover these costs or should the contractor estimate these as other direct costs? | There will be no other participants for which the contractor will need to recruit. The government will cover costs and has facilities. The contractor should not propose anything for this effort and incentives will not be paid. | NO | |
| 9 | Section 2 (Tasks), Subsection on support activities, page 44 | Will the government confirm that the "user research and design sessions" on this page are different from the usability testing sessions mentioned on page 42? Contractor presumes usability sessions test prototypes whereas the user research and design sessions are used to inform the design of concepts that would later be tested. | Confirmed. | NO | |

| | | | | |
|----|--|---|---|--|
| 10 | Section 2 (Tasks), Subsection on support activities, page 44 | The government states, "user research and design sessions" will occur several times each year and "each event may have multiple sessions." Can the government provide a number to be used for estimation purposes instead of "several"? What are the events? And will the government or the contractor be responsible for ODCs associated with facility rental and incentives for participants? | See response to question 8 | |
| 11 | PHASE 2 – Evaluation of Factor 1 Technical Challenge, Factor 3 Approach to Staffing and Factor 4 Price, Subsection on Factor 1 - Technical Challenge | In response to Question 21 in the "myUSCIS Draft RFP Responses to Questions-Comments.pdf related to the Draft RFP, the government stated, "Offerors may propose an innovative staffing approach. Their team that attends the Technical Challenge should be representative of the staffing approach for staffing the Agile teams . The challenge team should be based on the companies innovative approach and does not need to align to Attachment 4." Question: Does the reference to the technical challenge team being representative of the "Agile Teams" as stated indicate that the challenge team structure should align to the Agile Team structure proposed in Attachment 4, as opposed to some combination of the Technical Support Team and Agile Team? | No. | NO |
| 12 | PHASE 2 – Evaluation of Factor 1 Technical Challenge, Factor 3 Approach to Staffing and Factor 4 Price, Subsection on Factor 1 - Technical Challenge | In response to Question 103 in the "myUSCIS Draft RFP Responses to Questions-Comments.pdf related to the Draft RFP, the government stated, "No, the government will not be providing a user or product owner in the room. The government consciously took this approach because, as is reflected in Section M, an Offeror's ability to conduct user research is not something that we're evaluating during the Technical Challenge." Question: Can we assume based on the response to Question 103 in the Draft RFP QA response stating that there will not be a product owner or user representative in the room that there will be no direct interaction between the challenge team and the government during the challenge to clarify user stories, priorities, or discuss trade-off decisions between user needs, business goals, and technical feasibility? Can we also assume that in the absence of a product owner or user representative that all information necessary to execute the challenge from a business perspective will be included in the product vision? | Question Part 1. There will be no government product owner or user representative for direct interaction with the challenge team during the challenge to clarify user stories, priorities, discuss trade-off decisions between user needs, business goals, and technical feasibility. There will be an API technical resource in the room that will be available for clarification needs during the challenge.. | YES: updated technical challenge instructions page 58. |
| 13 | SOW Section 2 "Technical Lead Efforts" Page 39 | Bullet 4 is listed without a requirement. Is it intended to be left blank or deleted? | Deleted | YES: Removed the blank bullet. |
| 14 | | Please confirm that the average hourly rate range of \$182 to \$231 (based on the RFP dictated 1920 hours per year) to support the \$75m-95m government estimate is driven by staff resource quality, not by adding more than the prescribed 2 optional agile teams. | The hourly rate proposed shall be less than or equal to EAGLE II rates established. | NO |
| 15 | Evaluation and Selection, Page 61 | "The Government's design demonstration evaluation will evaluate the Offeror's design decisions, utilizing 3 of the following key areas, which are weighted equally" Question: Does USCIS expect offerors to ONLY talk to 3 of the 6 key areas? If offerors address all 6 areas across the 2 URLs, how will they be evaluated? | See response to question 4. | |
| 16 | Phase 2/Factor 1, Page 57 | " Use of tools is at the discretion of the vendor during the technical challenge. " Does the selection of a tool/technology rated in any way? Do the tools and technologies used on myuscis are preferred over other technologies? | Evaluation criteria is listed in section M. | NO |
| 17 | Phase 2 | " That information is expected to be related to user needs, business goals, and the APL." - Will the government provide fully functional API? Will the API be secured, and require authentication? How will the government provide documentaion for this API? | The government will provide an API for the Offeror to use during the Technical Challenge. More details on the Technical Challenge will be provided after Phase 1. | NO |
| 18 | Phase 2, Page 57 | "The government will notify offerors invited to Phase 2 seven (7) calendar days prior to their scheduled challenge date. " How many offeror does government plan to invite for phase 2? | Per the RFP "The most highly rated offers, with prices determined to be reasonable in phase 1, may proceed to participate in Phase 2 -Evaluation of Factors 1, 3 and 4." | NO |
| 19 | Phase 2, Page 57 | " The government plans to distribute details about the Technical Challenge after Phase 1, such as a product vision. " - Will the details be distributed right after phase 1 or to the demo invitees only 7 days before the demo? | Per the RFP "Along with the invitation for phase 2 the Government will supply details and needed information for the technical challenge." | NO |

| | | | | |
|----|--|---|---|---|
| 20 | Phase 2, Page 58 | "Offerors will be allowed to bring up to a maximum of 10 individuals to perform the technical challenge. " - do individuals who participate on in the demo have to be currently employed by Prime vendor or major subcontractors? | No | NO |
| 21 | General | Can the Government provide us with an estimated start date for the transition? | No we can not at this time. | NO |
| 22 | Part II Contract Clauses includes FAR 52.224-3 Privacy Training (JAN 2017) | Does the Government consider that the training requirements of Clause "HSAR Class Deviation 15-01 INFORMATION TECHNOLOGY SECURITY AND PRIVACY TRAINING (MAR 2015)" to satisfy the training requirements of FAR 52.224-3? | No | NO |
| 23 | Part II Contract Clauses includes FAR 52.224-3 Privacy Training (JAN 2017) | If Clause "HSAR Class Deviation 15-01 INFORMATION TECHNOLOGY SECURITY AND PRIVACY TRAINING (MAR 2015)" does not satisfy the training requirement for FAR 52.224-3, will the Government provide training to satisfy the requirements? | No | NO |
| 24 | Part IV - Instructions to Offerors Phase 1, Factor 2-Design Demonstration | For client confidentiality, we appreciate the opportunity to provide a demonstration site to show the work we have done for our clients. Please confirm that the Government requires the two submitted URL examples are representative of the sites that are current public facing sites. | Confirmed. Per RFP "The URL for the work example may link to the live site that resulted from the project or a link to a demonstration site that represents the work done on the project." | NO |
| 25 | Part IV - Instructions to Offerors Phase 2, Evaluation of Factor 1 Technical Challenge, Factor 3 Approach to Staffing and Factor 4 Price (pg 58) | The RFP reads "The government plans to distribute details about the Technical Challenge after Phase 1, such as a product vision." Given that the Technical Challenges are planned between July 25th - August 8th, please confirm that offerors will receive this information as they are invited to Phase 2, giving all offerors an equal amount of time with the additional details. | Per the RFP "Along with the invitation for phase 2 the Government will supply details and needed information for the technical challenge." All offerors will have the same amount of lead time. | NO |
| 26 | Part IV - Instructions to Offerors Phase 2, Evaluation of Factor 1 Technical Challenge, Factor 3 Approach to Staffing and Factor 4 Price (pg 59) | The RFP advises the offeror to arrive early enough to check the facility and validate the demonstration can begin on time. Is it possible to schedule a time before the day of the demonstration to check the facility to ensure that we bring all of the necessary equipment? If not, how early can we arrive on the day of the demonstration? | You may not check in the day before. You should show up approximately 30 minutes before. | NO |
| 27 | Part IV - Instructions to Offerors Phase 1, Factor 4 Price (pg 56) | Instructions in the RFP read "If the offer includes discounts from the parent contract's pricing rates, those discounts should be shown and explained in the business volume so the contracting officer can understand the basis for the discount." And " Offerors are encouraged to manipulate the sample staffing mix attachment #4 to provide the pricing". Is manipulating the attachment limited to inserting rows to populate additional roles? Please confirm that its acceptable for offerors to add a column and rows in Attachment 4 to show all requested information. | Offerors may adjust Attachment #4 as necessary to propose their price and staffing. | NO |
| 28 | Part IV - Instructions to Offerors Phase 1, Factor 4 Price (pg 56) | Instructions in the RFP require that pricing information be populated for each CLIN. Please confirm whether the offeror should add the B Table Summary as a tab in Attachment 4 or if it should be added as part of the Business Volume. | Offerors may adjust Attachment #4 as necessary to propose their price and staffing. | NO |
| 29 | Part IV - Instructions to Offerors Phase 1 Factor 2 Design Demonstration | The government indicated that the user name and passwords may not be provided. A design sample may include a registration and account section of the site to fully illustrate design capabilities relevant to MyUSCIS. For example, the government references "Nike Plus Membership web experience", which requires sign-up. Will the government evaluate self-registration as part of this experience? | The government will evaluate the evaluation factors listed in Section M. | No |
| 30 | Part IV - Instructions to Offerors Phase 2 Factor 1 Technical Challenge | The government indicates that individuals participating in the technical challenge are "not expected to be staffed on the myUSCIS task order." How will the government ensure that the quality of the team proposed is equivalent to the demonstrated capabilities of the team during the technical challenge? | This is not being evaluated by the government, and is provided for instruction purposes. only | NO |
| 31 | Part IV - Instructions to Offerors Phase 2 Factor 1 Technical Challenge | The role of the corporate representative is to observe team performance and will not perform in design, developing, deploying and demonstrating the MVP. This allows opportunities for the Corporate Representative to participate in the other Tech Challenge activities throughout the day. Please confirm that the Corporate Representative will be able to participate in the remaining activities, such as setup, team discussion during the tech challenge, explanation to evaluators, Demonstration preparation and Government Question Clarification. | That is an incorrect assumption. The role of the corporate representative is to observe team performance. | YES: Updated to read "...Corporate Representative who will be able to observe their team's performance and will not perform any technical challenge activities including, but not limited to, design, developing, deploying, and demonstrating the MVP. " |
| 32 | Schedule of Supplies/Services, Item No. 001 | Please confirm that QUANTITY represents months for all CLINS. | Confirm | NO |

| | | | | |
|----|--|---|---|--|
| 33 | Part IV - Instructions to Offerors Phase 1 Factor 2 Design Demonstration | How long will the government need access to the site for the URLs, video and technical demonstration site? | Up to award of the task order or longer if there is a protest. | NO |
| 34 | Part IV - Instructions to Offerors Phase 1 Factor 2 Design Demonstration | We assume the work sample should be interactive. What is meant by "demonstration site that represents work done on the project?" | Demonstration site means not the actual site, but a representative site for demonstration purposes. | NO |
| 35 | Part IV - Instructions to Offerors Phase 2 Factor 1 Technical Challenge | Will there be any interaction during the challenge with on-site product owner and/or end user? Question 103 from the draft Q&A stated no user or PO would be in the room but the final RFP does not mention that. | See response to question 12 | |
| 36 | Part IV - Instructions to Offerors Phase 2 Factor 1 Technical Challenge | Please confirm the Technical Challenge invitation will include use case information from which the Offeror can determine the skills and capabilities needed on the day of the Technical Challenge. | Additional details about the Tech Challenge will be provided after Phase 1. | NO |
| 37 | Part III - Documents, exhibits, or attachments, 1.Scope of Work (P.37, Item 7) | 2. P.37, Item 7: The government directs the contractor to provide four teams in the Base Period and five teams in the Option periods as a minimum capacity to meet its objectives. Two additional optional teams are directed providing additional support. Please confirm that the stated teams are the required basis of estimate for the Offeror's price. From the RFP - "6. USCIS is focused on the goal of eProcessing by 2020, and since we still have over 100 forms to bring online.. An implementation plan is not currently available for the eProcessing, however, USCIS may need additional services (optional CLINS) to meet the deadline set forth by the USCIS Leadership. Those additional services are expected to be completed under the optional CLINs for additional teams. 7. The contractor shall provide the Government with four Agile teams during the base period, and if exercised two additional optional teams. The contractor shall provide the Government with five Agile teams during each of the option periods, and if exercised two additional optional teams. (Reference Sample Staffing Mix Attachment #4). Additional teams are required through optional CLINS to allow the Government to receive additional support." | Confirmed | NO |
| 38 | Part IV - Instructions to Offerors Phase 2, Factor 3 Approach to Staffing and Factor 4 Price (pg 59) | In order to provide sufficient context and rationale for our staffing approach, we request that the PDF document be limited to 3 pages rather than 2 pages. Please confirm that the Approach to Staffing explanation can be 3 pages using 10 point font. | The approach to staffing PDF document limit is increased to a total of 5 pages (which includes the cover page). | YES: Updated Factor descriptions on pages 54/60 and approach to staffing instructions page 59. |
| 39 | Expectation Regarding Agile Teams (pg. 12); Staffing Attachment 4 | Is it the Government's intent that (a) the total number of FTES for Agile Teams on CLIN 0002 (Base Tab, lines 16-19) must equal at least 40, and (b) the total number of FTES for all Optional Agile Teams (CLINs 0004 and 0005) must equal at least 10 FTES per team? | Confirmed | |
| 40 | Phase 2 Evaluation, Factor 3 - Approach to Staffing (pg. 60) | To avoid giving offerors with DCAA-approved FPRAs an unfair price advantage, will the Government allow offerors to utilize 1,880 hours as a full-time productive equivalent, rather than the 1,920 as dictated by the Solicitation? | The government has not dictated the full time equivalent to be 1,920 hr. Per the RFP "A full time equivalent in Attachment #4 assumes 1,920 hours annum. Contractors SHALL NOT provide the assumption for hours for an FTE, the Government is only providing it to further support the contractors understanding of the sample staffing levels. Contractors SHALL NOT propose hours, rather propose FTE team composition. If contractors are proposing less than a full time person (i.e. less than 1,920 hours in Attach 1) they may propose to the 10 th (for example: .5 FTE, .3 FTE). The Government does not need to know or understand the hour's annum buildup for the FTE's proposed. | NO |
| 41 | Instructions, B (pg. 54) | Please confirm that Phase 1 deliverables (Factors 2 and 4) are due on the proposal due date (June 19, 2018 at 2:00 PM EST). | Confirmed | NO |
| 42 | Page 52, 52.216-1 | Please confirm that the Government intends to award a contract to a single offeror as a result of this solicitation. | Confirmed a single award is anticipated. | NO |
| 43 | Instructions to Offerors | Does the government require the URLs for the Design Demonstration examples to be submitted in an MS Word document as perhaps Volume 1 - Technical Challenge, or just include the links to the URLs in the body of the email with the Business Volume as the only attachment with the email submission? | The URLs shall be provided in the written response email to the email addresses listed in the RFP. | YES: Updated Factor 2 instructions page 56 |
| 44 | Solicitation, SF1447 Continuation Sheet | Are Offerors required to complete and submit the SF1447 Continuation Sheet CLIN tables as part of its Factor 4 - Price / Business Volume submission? | This is not a requirement. Pricing shall be submitted on Attachment #4. | NO |
| 45 | Instructions to Offerors | After notification of an invitation for phase 2 and the Government provides details for the technical challenge, will the Government provide an opportunity to clarify any questions prior to the Technical Challenge? | No. There will not be an additional opportunity for questions. | NO |

| | | | | |
|----|--|--|--|---|
| 46 | Instructions to Offerors, Factor 1 Technical Challenge | The RFP states, "For the technical challenge, the Offeror shall design, develop, and deploy an application to a cloud environment. The details and needed information for the technical challenge will be supplied along with the invitation to the vendor for Phase 2." Are offerors permitted to begin Technical Challenge set-up activities (e.g., AWS environment configuration) when initially notified of participation? | Per the RFP "Offerors are not required to start from scratch on the day of the Technical Challenge. The government plans to distribute details about the Technical Challenge after Phase 1, such as a product vision." How much to set up before the Tech Challenge is at the discretion of the Offeror. Starting from scratch is allowed and so is pre-fabrication. | NO |
| 47 | Instructions to Offerors, Factor 1 Technical Challenge | The RFP states, "The Offeror shall use a modern technical development stack, tools, and CI/CD pipeline to design, develop, and deploy the application," Can an offerors technical challenge stack, tools, and CI/CD pipeline include elements not used by USCIS? | Yes | NO |
| 48 | Instructions to Offerors, Factor 1, Technical Challenge | The RFP states, "The Offeror's MVP demonstration will allow the Government to experience the MVP produced by the Offeror and to hear the rationale behind the Offeror's decision-making in designing, developing, and deploying the MVP." Will there be a projection/display screen available in the conference room the contractors can use as part of their MVP product demo? | The government will simply be providing a room, that is expected to be a normal conference room. | YES: updated instructions to offerors, pg 59, to read : "The vendor must provide their own equipment for the technical challenge, including but not limited to, internet access and any supplies needed (sticky notes, computer, food, drinks, etc.). " |
| 49 | Instructions to Offerors | Should the document containing Factor 4 - Price be titled "Business Volume"? | Yes | NO |
| 50 | Instructions to Offerors, Approach to Staffing (Phase 2) and Factor 4 – Price (Phase 1 & 2) | Is the same Attachment # 4, myUSCIS Government Sample Staffing Mix and CLIN Structure spreadsheet, to be completed for both Factor 3 - Approach to Staffing (Phase 2) as well as for Factor 4 – Price (Phase 1 & 2)? | Staffing Mix and pricing are provided on attachment #4 during phase 1 (only submitted once) Pricing will be evaluated in phase 1 and phase 2. Factor 3 - Approach to Staffing additional documentation (5 page PDF supporting rational) shall be submitted in phase 2. | YES: Updated instructions to offerors Factor 3, page 60 |
| 51 | Phase 1 - Evaluation of Factors 2 and 4 | Please confirm that USCIS will provide the Rating for Factor 2 as evaluated in Phase 1, when the vendor is notified of its participation in Phase 2. | At the conclusion of phase 1 the offer will be notified if they among the most highly rated offerors invited to phase 2. The offeror will not be provided their individual rating until post award debriefings, if requested. | NO |
| 52 | Phase 1 - Evaluation of Factors 2 and 4 | Please confirm if the Phase 1 step is an "Advisory" step - i.e. will the offeror receive an Advisory Notification that it will be invited to participate in the resultant acquisition or, based on the information submitted, that it is unlikely to be a viable competitor. | Per the RFP phase 1 "is a mandatory firm down-select." | NO |
| 53 | Continuation Page 3, 4 CLINs X004, X005 Page 12 - Expectation Regarding Agile Teams Phase 1 - Evaluation of Factors 2 and 4 Factor 4 - Price Pg 59 | Team of 10 FTEs "The Government's expectation is that the Contractor's Agile Teams will continuously provide at least 10 FTEs of IT professionals ...to achieve the Government's needs ..." "Populated pricing information for each CLIN. Offerors are encouraged to manipulate the sample staffing mix attachment #4 to provide the pricing. This spreadsheet includes the labor categories proposed and number of FTEs, therefore, contractors can simply insert the proposed pricing for each CLIN." Offeror's are not encouraged to copy sample staffing mix, but should propose their own innovative staffing composition. When proposing their staffing mix, Offerors shall adjust the spreadsheet as necessary to fit their proposal , while maintaining the CLIN structure organization, as pricing shall be provided that aligns to the CLIN structure. Please confirm the vendor can use its best judgment to determine the team size (i.e. # FTEs) and labor mix which the vendor estimates to be the most effective, possibly even less than 10 FTEs.. | The vendor's assumption is incorrect. Please see question 39 and response. The government is not evaluating the size of teams in the staffing approach. The government is only evaluating the labor mix. The RFP has been updated to read that the level of effort is established and only the labor mix will be evaluated. | YES: updated evaluation of factor 3 to read: "The approach to staffing will be evaluated as Outstanding, Good Acceptable, or Unacceptable. The Government will evaluate labor mix proposed (FTEs NOT hours), as the level of effort has been established, and supporting rationale for how the contractor understands the SOW and will successfully perform the task order requirements." |
| 54 | N/A | Has the Procurement Innovation Lab (PIL) influenced the acquisition approach? If so, please indicate where that influence was included. | This is not relevant to the evaluation or procurement. | NO |
| 55 | SF 1447 | To ensure the pricing is as reasonable as possible, would you consider extending the Phase 1 proposal due date by one (1) week? | The due date for submissions will be extended by 2 days. Proposals will now be due on June 21, 2018 by 2:00pm EST. | YES |
| 56 | Factor 1 – Technical Challenge | The SOW stipulates "Use of tools is at the discretion of the vendor during the technical challenge" and "The team attending the technical challenge is expected to be representative of what the Offeror would provide the Government after contract award." Please confirm that the environment used to develop the MVP during the technical challenge is not going to be part of the evaluation. | Confirmed. Offerors will be evaluated in accordance with the evaluation criteria in the solicitation. | NO |
| 57 | Factor 1 – Technical Challenge | The SOW states: "The Government shall be able to access e-artifacts, code repositories and tools from current Government furnished equipment rather than vendor supplied equipment." What is the preferred method for Government access to the systems, artifacts, code repositories and tools used by the vendor for the technical challenge? | There is no preferred method. Per the RFP "The Offeror shall provide the Government real-time access to any and all systems utilized by the vendors for the challenge including but not limited to artifacts, code repositories and tools used." | NO |

| | | | | |
|----|--|---|---|----|
| 58 | Instructions to Offerors on page 55 | Will the government accept the submission of websites that require a password if they are USCIS sites? | No. | NO |
| 59 | Final RFP 70SBUR18R0000020 Instructions to Offerors Factor 4 Page 56 | Software exists that could be used to lower the cost of labor and thus should be allowed and evaluated. Please amend the RFP to include an ODC CLIN for software. | Offerors will be evaluated in accordance with the evaluation criteria in the solicitation. No ODC for software will be added. | NO |
| 60 | Final RFP 70SBUR18R0000020 Part II Contract Clauses 3052.215-70 Key Personnel or Facilities Page 9 | Can the Government please either provide a section in the Staffing Attachment 4 or allow a resume submitted in part Part I to highlight the qualifications of our proposed Program Manager Key. | See response to question 7 | |
| 61 | Instructions to Offerors on page 55 | Does the publicly accessible URLs allowing the Government to view the actual products designed by the Offeror need to be placed in the 5 minute video or embedded in the written response? | See response to question 44 | |