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

| 1. REQUISITION NUMBER | PAGE | OF |
|---|---|---|
| Multiple | 1 | 4 |

| 2. CONTRACT NO. | 3. AWARD/ EFFECTIVE DATE | 4. ORDER NUMBER | 5. SOLICITATION NUMBER | 6. SOLICITATION ISSUE DATE |
|---|---|---|---|---|
| GS-35F-135BA | | HSSCCG-16-F-00619 | HSSCCG-16-Q-00405 | 09/08/2016 |

| 7. FOR SOLICITATION INFORMATION CALL: | a. NAME | b. TELEPHONE NUMBER (No collect calls) | 8. OFFER DUE DATE/LOCAL TIME |
|---|---|---|---|
| | EMILIO CIBULA | 802-872-4111 | |

| 9. ISSUED BY | CODE | 10. THIS ACQUISITION IS |
|---|---|---|
| USCIS Contracting Office<br>Department of Homeland Security<br>70 Kimball Avenue<br>South Burlington VT 05403 | CIS | ☐ UNRESTRICTED OR ☒ SET ASIDE % FOR:<br>☒ SMALL BUSINESS<br>☐ HUBZONE SMALL BUSINESS<br>☒ SERVICE-DISABLED VETERAN-OWNED SMALL BUSINESS<br>☐ WOMEN-OWNED SMALL BUSINESS (WOSB) ELIGIBLE UNDER THE WOMEN-OWNED SMALL BUSINESS PROGRAM<br>☐ EDWOSB<br>☐ 8(A)<br>NAICS: 541519<br>SIZE STANDARD: 150 |

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

| 15. DELIVER TO | CODE | 16. ADMINISTERED BY | CODE |
|---|---|---|---|
| Department of Homeland Security<br>US Citizenship & Immigration Svcs<br>Office of Information Technology<br>111 Massachusetts Ave, NW<br>Suite 5000<br>Washington DC 20529 | HQOIT | USCIS Contracting Office<br>Department of Homeland Security<br>70 Kimball Avenue<br>South Burlington VT 05403 | CIS |

| 17a. CONTRACTOR/ OFFEROR | CODE | FACILITY CODE | 18a. PAYMENT WILL BE MADE BY | CODE |
|---|---|---|---|---|
| JHC TECHNOLOGY INC<br>ATTN JHC TECHNOLOGY INC<br>401 POST OFFICE RD<br>SUITE 201<br>WALDORF MD 206023225<br><br>TELEPHONE NO. | 9618097900000 | | See Invoicing Instructions | WEBVIEW |

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

18b. SUBMIT INVOICES TO ADDRESS SHOWN IN BLOCK 18a UNLESS BLOCK BELOW IS CHECKED ☐ SEE ADDENDUM

| 19. ITEM NO. | 20. SCHEDULE OF SUPPLIES/SERVICES | 21. QUANTITY | 22. UNIT | 23. UNIT PRICE | 24. AMOUNT |
|---|---|---|---|---|---|
| | DUNS Number: 961809790+0000<br>---<br>AWS Cloud Hosting (IaaS)<br>---<br>Schedule of Attachments:<br>1. Award Terms + Conditions & Clauses;<br>2. Final Statement of Work;<br>*(Use Reverse and/or Attach Additional Sheets as Necessary)* | | | | |

| 25. ACCOUNTING AND APPROPRIATION DATA | 26. TOTAL AWARD AMOUNT *(For Govt. Use Only)* |
|---|---|
| See schedule | $[redacted] |

☐ 27a. SOLICITATION INCORPORATES BY REFERENCE FAR 52.212-1, 52.212-4. FAR 52.212-3 AND 52.212-5 ARE ATTACHED. ADDENDA ☐ ARE ☐ ARE NOT ATTACHED.

☐ 27b. CONTRACT/PURCHASE ORDER INCORPORATES BY REFERENCE FAR 52.212-4. FAR 52.212-5 IS ATTACHED. ADDENDA ☐ ARE ☐ ARE NOT ATTACHED.

☐ 28. CONTRACTOR IS REQUIRED TO SIGN THIS DOCUMENT AND RETURN _____ COPIES TO ISSUING OFFICE. CONTRACTOR AGREES TO FURNISH AND DELIVER ALL ITEMS SET FORTH OR OTHERWISE IDENTIFIED ABOVE AND ON ANY ADDITIONAL SHEETS SUBJECT TO THE TERMS AND CONDITIONS SPECIFIED.

☐ 29. AWARD OF CONTRACT: _____ OFFER DATED _____. YOUR OFFER ON SOLICITATION (BLOCK 5), INCLUDING ANY ADDITIONS OR CHANGES WHICH ARE SET FORTH HEREIN, IS ACCEPTED AS TO ITEMS:

| 30a. SIGNATURE OF OFFEROR/CONTRACTOR | 31a. UNITED STATES OF AMERICA *(SIGNATURE OF CONTRACTING OFFICER)* |
|---|---|
| | Chad B Pa |

| 30b. NAME AND TITLE OF SIGNER *(Type or print)* | 30c. DATE SIGNED | 31b. NAME OF CONTRACTING OFFICER *(Type or print)* | 31c. DATE SIGNED |
|---|---|---|---|
| | | Chad Parker | 9/29/2016 |

AUTHORIZED FOR LOCAL REPRODUCTION
PREVIOUS EDITION IS NOT USABLE

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

| 19. ITEM NO. | 20. SCHEDULE OF SUPPLIES/SERVICES | 21. QUANTITY | 22. UNIT | 23. UNIT PRICE | 24. AMOUNT |
|---|---|---|---|---|---|
| | 3. Statement of Work Attachment 1 - Security Language;<br>4. PII Language;<br>5. Security Clause 3.<br>AAP Number: N/A DO/DPAS Rating: NONE<br>Period of Performance: 09/30/2016 to 09/29/2017 | | | | |
| 0001 | AWS IaaS (FFP)<br><br>Accounting Info:<br>VISAWS1 000 QB 70-01-00-000<br>07-20-0200-00-00-00-00 GE-25-86-00 000000<br>Funded: $[redacted]<br>Accounting Info:<br>ITALM00 000 EX 20-01-00-000<br>23-20-0200-00-00-00-00 GE-25-47-00 000000<br>Funded: $[redacted]<br>Accounting Info:<br>ITFACLE PM0 EX 20-01-00-000<br>23-20-0400-00-00-00-00 GE-25-41-00 000000<br>Funded: $[redacted]<br>Accounting Info:<br>ITCSPRT ACS EX 20-05-00-000<br>23-20-0600-00-00-00-00 GE-25-86-00 000000<br>Funded: $[redacted]<br>Accounting Info:<br>ITENTSR ESB EX 20-05-00-000<br>23-20-0600-00-00-00-00 GE-25-86-00 000000<br>Funded: $[redacted]<br>Continued ... | 1 | LO | [redacted] | [redacted] |

32a. QUANTITY IN COLUMN 21 HAS BEEN

☐ RECEIVED ☐ INSPECTED ☐ ACCEPTED, AND CONFORMS TO THE CONTRACT, EXCEPT AS NOTED: _____

| 32b. SIGNATURE OF AUTHORIZED GOVERNMENT REPRESENTATIVE | 32c. DATE | 32d. PRINTED NAME AND TITLE OF AUTHORIZED GOVERNMENT REPRESENTATIVE |
|---|---|---|
| | | |

| 32e. MA LING ADDRESS OF AUTHORIZED GOVERNMENT REPRESENTATIVE | 32f. TELEPHONE NUMBER OF AUTHORIZED GOVERNMENT REPRESENTATIVE<br>32g. E-MA L OF AUTHORIZED GOVERNMENT REPRESENTATIVE |
|---|---|
| | |

| 33. SHIP NUMBER<br>☐ PARTIAL ☐ FINAL | 34. VOUCHER NUMBER | 35. AMOUNT VERIFIED CORRECT FOR | 36. PAYMENT<br>☐ COMPLETE ☐ PARTIAL ☐ FINAL | 37. CHECK NUMBER |
|---|---|---|---|---|
| | | | | |

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

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

| ITEM NO. (A) | SUPPLIES/SERVICES (B) | QUANTITY (C) | UNIT (D) | UNIT PRICE (E) | AMOUNT (F) |
|---|---|---|---|---|---|
| | Accounting Info:<br>ITRECOR NFT EX 20-04-00-000<br>23-20-0600-00-00-00-00 GE-25-86-00 000000<br>Funded: $[redacted]<br>Accounting Info:<br>ITDCS00 DCN EX 20-01-00-000<br>23-20-0400-00-00-00-00 GE-25-41-00 000000<br>Funded: $[redacted]<br>Accounting Info:<br>ITPCLOU 000 EX 20-05-00-000<br>23-20-0500-00-00-00-00 GE-25-14-00 000000<br>Funded: $[redacted] | | | | |
| 0002 | AWS IaaS Surge Up To 20% (Optional)<br>Amount: $[redacted] (Option Line Item)<br>Anticipated Exercise Date:01/01/0001<br><br>Accounting Info:<br>Funded: $[redacted] | 1 | LO | [redacted] | [redacted] |
| 0003 | AWS Cloudability (FFP)<br><br>Accounting Info:<br>VISAWS1 000 QB 70-01-00-000<br>07-20-0200-00-00-00-00 GE-25-86-00 000000<br>Funded: $[redacted] | 1 | EA | [redacted] | [redacted] |
| 0004 | TWILIO (FFP)<br><br>Accounting Info:<br>VISAWS1 000 QB 70-01-00-000<br>07-20-0200-00-00-00-00 GE-25-86-00 000000<br>Funded: $[redacted] | 1 | EA | [redacted] | [redacted] |
| 1001 | AWS IaaS (FFP)<br>Amount: $[redacted] (Option Line Item)<br>Anticipated Exercise Date:03/29/2017 | 1 | LO | [redacted] | [redacted] |
| 1002 | AWS IaaS Surge Up To 20% (Optional)<br>Amount: $[redacted] (Option Line Item)<br>Anticipated Exercise Date:03/29/2017 | 1 | LO | [redacted] | [redacted] |
| 1003 | AWS Cloudability (FFP)<br>Amount: $[redacted] (Option Line Item)<br>Anticipated Exercise Date:04/01/2016<br>Continued ... | 1 | EA | [redacted] | [redacted] |

| ITEM NO. (A) | SUPPLIES/SERVICES (B) | QUANTITY (C) | UNIT (D) | UNIT PRICE (E) | AMOUNT (F) |
|---|---|---|---|---|---|
| 1004 | TWILIO (FFP)<br>Amount: $[redacted] (Option Line Item)<br>Anticipated Exercise Date:04/01/2016<br><br>The following are Administrative Points of Contact for this order:<br><br>Contracting Officer's Representative (COR):<br>Robyn J. Zellars<br>Phone: (202) 272-8608<br>Email: Robyn.J.Zellars@USCIS.DHS.GOV<br><br>Contract Specialist (CS):<br>Emilio A. Cibula<br>Phone (802) 872-4640<br>Email: Emilio.A.Cibula@USCIS.DHS.GOV<br><br>Contracting Officer (CO):<br>Heather V. Niquette<br>Phone: (802) 872-4661<br>Email: Heather.V.Niquette@USCIS.DHS.GOV<br><br>The total amount of award: $[redacted]. The obligation for this award is shown in box 26. | 1 | EA | [redacted] | [redacted] |

U.S. Citizenship and Immigration Services
*Office of Contracting*
70 Kimball Ave
South Burlington VT 05403

U.S. Citizenship and Immigration Services

**II. Line Item Structure**

Amazon services are to be provided on a fixed-unit-price (FUP) basis and the individual services provided by Amazon are too voluminous to list in the CLIN structure. The FFP price is a Not- To Exceed (NTE) amount. The government understands this is a pay per use service; therefore, monthly invoices will fluxuate based on government usage along with FUP price fluxuations from Amazon. The contractor shall and the government will track the spend rates to ensure the contractor does not exceed the FFP amounts. Should we reach the FFP NTE amounts the government may exercise surge CLINs for additional services.

**III. Task Order Clauses & Other Terms of the Order**

**Homeland Security Acquisition Regulation (HSAR) clauses incorporated by reference**

- HSAR 3052.205-70, Advertisements, Publicizing Awards, and Releases (SEP 2012)
- HSAR 3052.242-72, Contracting Officer's Representative (DEC 2003)

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

**HSAR 3052.209-70 PROHIBITION ON CONTRACTS WITH CORPORATE EXPATRIATES**

**(JUN 2006)**

(a) Prohibitions.

Section 835 of the Homeland Security Act, 6 U.S.C. 395, prohibits the Department of Homeland Security from entering into any contract with a foreign incorporated entity which is treated as an inverted domestic corporation as defined in this clause, or with any subsidiary of such an entity. The Secretary shall waive the prohibition with respect to any specific contract if the Secretary determines that the waiver is required in the interest of national security.

(b) Definitions. As used in this clause:

*Expanded Affiliated Group* means an affiliated group as defined in section 1504(a) of the Internal Revenue Code of 1986 (without regard to section 1504(b) of such Code), except

that section 1504 of such Code shall be applied by substituting `more than 50 percent' for `at least 80 percent' each place it appears.

*Foreign Incorporated Entity* means any entity which is, or but for subsection (b) of section 835 of the Homeland Security Act, 6 U.S.C. 395, would be, treated as a foreign corporation for purposes of the Internal Revenue Code of 1986.

*Inverted Domestic Corporation.* A foreign incorporated entity shall be treated as an inverted domestic corporation if, pursuant to a plan (or a series of related transactions)—

(1) The entity completes the direct or indirect acquisition of substantially all of the properties held directly or indirectly by a domestic corporation or substantially all of the properties constituting a trade or business of a domestic partnership;

(2) After the acquisition at least 80 percent of the stock (by vote or value) of the entity is held—

(i) In the case of an acquisition with respect to a domestic corporation, by former shareholders of the domestic corporation by reason of holding stock in the domestic corporation; or

(ii) In the case of an acquisition with respect to a domestic partnership, by former partners of the domestic partnership by reason of holding a capital or profits interest in the domestic partnership; and

(3) The expanded affiliated group which after the acquisition includes the entity does not have substantial business activities in the foreign country in which or under the law of which the entity is created or organized when compared to the total business activities of such expanded affiliated group.

*Person, domestic, and foreign* have the meanings given such terms by paragraphs (1), (4), and (5) of section 7701(a) of the Internal Revenue Code of 1986, respectively.

(c) Special rules. The following definitions and special rules shall apply when determining whether a foreign incorporated entity should be treated as an inverted domestic corporation.

(1) *Certain stock disregarded.* For the purpose of treating a foreign incorporated entity as an inverted domestic corporation these shall not be taken into account in determining ownership:

(i) Stock held by members of the expanded affiliated group which includes the foreign incorporated entity; or

(ii) Stock of such entity which is sold in a public offering related to an acquisition described in section 835(b)(1) of the Homeland Security Act, 6 U.S.C. 395(b)(1).

(2) *Plan deemed in certain cases*. If a foreign incorporated entity acquires directly or indirectly substantially all of the properties of a domestic corporation or partnership during the 4-year period beginning on the date which is 2 years before the ownership requirements of subsection (b)(2) are met, such actions shall be treated as pursuant to a plan.

(3) *Certain transfers disregarded*. The transfer of properties or liabilities (including by contribution or distribution) shall be disregarded if such transfers are part of a plan a principal purpose of which is to avoid the purposes of this section.

(d) *Special rule for related partnerships*. For purposes of applying section 835(b) of the Homeland Security Act, 6 U.S.C. 395(b) to the acquisition of a domestic partnership, except as provided in regulations, all domestic partnerships which are under common control (within the meaning of section 482 of the Internal Revenue Code of 1986) shall be treated as a partnership.

(e) Treatment of Certain Rights.

(1) Certain rights shall be treated as stocks to the extent necessary to reflect the present value of all equitable interests incident to the transaction, as follows:

(i) warrants;

(ii) options;

(iii) contracts to acquire stock;

(iv) convertible debt instruments; and

(v) others similar interests.

(2) Rights labeled as stocks shall not be treated as stocks whenever it is deemed appropriate to do so to reflect the present value of the transaction or to disregard transactions whose recognition would defeat the purpose of Section 835.

(f) *Disclosure.* The offeror under this solicitation represents that [Check one]:

__ it is not a foreign incorporated entity that should be treated as an inverted domestic corporation pursuant to the criteria of (HSAR) 48 CFR 3009.108-7001 through 3009.108-7003;

__ it is a foreign incorporated entity that should be treated as an inverted domestic corporation pursuant to the criteria of (HSAR) 48 CFR 3009.108-7001 through 3009.108-

7003, but it has submitted a request for waiver pursuant to 3009.108-7004, which has not been denied; or

__ it is a foreign incorporated entity that should be treated as an inverted domestic corporation pursuant to the criteria of (HSAR) 48 CFR 3009.108-7001 through 3009.108-7003, but it plans to submit a request for waiver pursuant to 3009.108-7004.

(g) A copy of the approved waiver, if a waiver has already been granted, or the waiver request, if a waiver has been applied for, shall be attached to the bid or proposal.

(End of clause)

**HSAR 3052.204-71 CONTRACTOR EMPLOYEE ACCESS (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.

(End of clause)

**HSAR 3052.204-71 CONTRACTOR EMPLOYEE ACCESS ALTERNATE I (SEP 2012)**

When the contract will require contractor employees to have access to Information Technology (IT) resources, add the following paragraphs:

a. 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.

b. The contractor shall have access only to those areas of DHS information technology resources explicitly stated in this contract or approved by the COTR in writing as

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

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

c. 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.

d. 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.

e. Contractors shall identify in their quotes 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)

**Other Task Order Terms**

All of the contractor's GSA Schedule contract clauses/terms and conditions are applicable to the resultant task order. Reference GSA IT 70 Schedule (GS-35F-135BA).

**1. Delivery**

Delivery Date: The Amazon Web Services cloud access shall be provided within one (1) day from the time of the award. Unrestricted data access shall be provided for the following e-mail destinations:

[redacted].

**Contractor POC:**

Matt Jordan, Vice President
mjordan@jhctechnology.com
814-421-0617
401 Post Office Road, Suite 201
Waldorf, Md., 20602
jhctechnology.com

**2. Performance Reporting**

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

**3. Invoice Requirements**

(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**

**4. 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 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.

**5. FOIA Posting**

The Government intends to post the contract/order to the FOIA reading room. The contractor shall provide a redacted copy of the order including attachments suitable for public posting within 30 days of award.

**6. Contractor Discounts and Assumptions**

Standard GSA Discounts for Nos. 1 and 2 apply to AWS Infrastructure services only, however Nos. 3 and 4 apply to labor and infrastructure.

1. 1% discount per task/delivery order from $0-$99,999
2. 2% discount per task/delivery order from $100,000+
3. Prompt Payment: 2%, 20 days from receipt of invoice or date of acceptance, whichever comes first
4. Credit Card Discount of 1%, 10 days
5. [redacted]
6. The Government has requested a separate breakout of the support/overhead cost. JHC will provide [redacted] at [redacted]. Given the totals for the CLIN 0001 and 1001, JHC's FFP pricing is as follows: Base Period: [redacted] / Option Period: [redacted].
7. Other quote assumptions are as follows:

| usage type | Assumptions |
|---|---|
| DataTransfer-Regional-Bytes | [redacted] |
| All | [redacted] |
| BoxUsage:m3.medium; Boxusage:m4.xlarge; BoxUsage:m3.2xlarge | [redacted] |
| EBS:VolumeUsage.gp2 | [redacted] |
| Standard Storage | [redacted] |

| | |
|---|---|
| Standard IA Storage | [redacted] |
| Reduced RR Storage | |
| InstanceUsage:db.m3.2xlarge | |
| VPC Data in (GB/mo | |

# USCIS Amazon Web Services (AWS) Infrastructure as a Service (IaaS) Statement of Work (SOW)

## 1.0. Background

Amazon Web Services (AWS) is a comprehensive, evolving cloud computing platform provided by Amazon.com. Web services are sometimes called cloud services.

## 2.0. Scope

The U.S. Citizen Immigration Services (USCIS) Office of Information Technology requires Amazon Web Services (AWS) Infrastructure as a Service (IaaS). The contractor and Amazon will provide all the hardware and a virtualization platform so USCIS can spin up information on the cloud. The contractor shall provide access to all the Amazon Services available to the commercial market. The growing AWS collection offers over three dozen diverse services and all AWS offerings are billed according to usage and the Fixed Unit Prices (FUP) are attached to this order. The Contractor shall provide the USCIS Amazon Web Services (AWS) Infrastructure Services on the Amazon Commercial Cloud.

This service shall include, application hosting, which is a virtualization platform for USCIS to upload our systems along with a web server and application intelligence. For example, ELIS is a USCIS application that sits on top of virtualization infrastructure. Automated performance monitoring is also required, which are commercial services available with the web-services package. This service shall also include continuous integration and deployment systems, which are unique, as the amazon API services must be compatible and automated to work with the USCIS environment. Lastly, the requirement includes data analytics products and Cloud Cost Tracking Services.

The IaaS shall be flexible and scalable, which means USCIS must be able to create or destroy infrastructure at will. It must also be automated, cost-effective, with secure IT infrastructure. It must be able to support the agile delivery of IT capabilities to the USCIS stakeholders. USCIS requires these services for existing USCIS systems like ELIS, which is already in the AWS cloud, and new programs, systems, and IT capabilities implemented by the Agency, in addition to legacy information systems migrating to cloud-based IT support models. USCIS programs and systems supported by this SOW can serve both public and private stakeholders and can range broadly in terms of size, complexity and importance.

The contractor shall provide the following services in support of the IAAS services.

1. Provisioning of accounts, including collection of USCIS user information; management of the Master Payer Account. Organization of the accounts in the console and reporting/analysis tools.
2. Collection, analysis, and synthesis of Agency usage for all services provided by the contractor to ensure accurate billing through Cloudability.

3. The contractor shall provide licensing and TWILIO messaging service that is a key part of our customer authentication mechanism.
4. The contractor shall provide a Technical point of contact for account management.
5. The contractor shall provide a web portal to submit service tickets, track request progress, and resolution status. This should be used for new account requests, and decommissioning of accounts if necessary.
6. The contractor shall provide a method to receive and forward account alerts from AWS – Maintenance notifications, AMI termination, etc to the USCIS account manager.
7. The contractor shall provide the capability to create AWS accounts, setup IAM users, and assign the user a role.
8. The contractor shall provide the capability to create access keys to an IAM and perform initial setup of and integration between cost management software and AWS.
9. The contractor shall provide the capability to managed linked accounts under a central billing account model.
10. The contractor shall provide the ability for USCIS to manage Cloudability tool.
11. The contractor shall provide the ability for the customer (USCIS) to maintain full control over the account, to create, stop or terminate any service offered by AWS in the account unimpeded. The contractor shall not impose any restriction for USCIS to utilize services in the account(s). The government must have full control to create instances in the account. The contractor shall not implement change control processes which that the Government's ability to utilize AWS.
12. The contractor shall ensure that no resources or services are created in the combined billing account, excluding S3.
13. The contractor shall support transition on the master payer account to the new contractor. Each linked account shall be moved under the new master payer account and there shall be no disruption of service. The government also requires a new Cloudability account, which requires the creation of new access keys once the account is built.

## 2.1 Deliverables

The contractor holds the root payer account for Amazon and the contractor is reimbursed for amounts paid to Amazon. The contractor shall provide access to the Amazon network within one business day of award.

The contractor addresses account access and notifications; therefore, the contractor shall provide account notifications as they arise.

The Government intends to post the contract/order to the FOIA reading room. The contractor shall provide a redacted copy of the order including attachments suitable for public posting within 30 days of award.

**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.

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.

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.

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:
Data Universal Numbering System (DUNS);
Contract numbers affected unless all contracts by the company are affected;
Facility CAGE code if the location of the event is different than the prime contractor location;
Point of contact (POC) if different than the POC recorded in the System for Award Management (address, position, telephone, email);
Contracting Officer POC (address, telephone, email);
Contract clearance level;
Name of subcontractor and CAGE code if this was an incident on a subcontractor network;
Government programs, platforms or systems involved;
Location(s) of incident;
Date and time the incident was discovered;
Server names where sensitive information resided at the time of the incident, both at the Contractor and subcontractor level;
Description of the Government PII and/or SPII contained within the system;
Number of people potentially affected and the estimate or actual number of records exposed and/or contained within the system; and
Any additional information relevant to the incident.

(g) Sensitive Information Incident Response Requirements.

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.
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.
Incident response activities determined to be required by the Government may include, but are not limited to, the following:
Inspections,
Investigations,
Forensic reviews, and
Data analyses and processing.
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.
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:
A brief description of the incident;
A description of the types of PII and SPII involved;
A statement as to whether the PII or SPII was encrypted or protected by other means;
Steps individuals may take to protect themselves;
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
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:
Provide notification to affected individuals as described above; and/or

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:
Triple credit bureau monitoring;
Daily customer service;
Alerts provided to the individual for changes and fraud; and
Assistance to the individual with enrollment in the services and the use of fraud alerts; and/or establish a dedicated call center. Call center services shall include:
A dedicated telephone number to contact customer service within a fixed period;
Information necessary for registrants/enrollees to access credit reports and credit scores;
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;
Escalation of calls that cannot be handled by call center staff to call center management or DHS, as appropriate;
Customized FAQs, approved in writing by the Contracting Officer in coordination with the Headquarters or Component Chief Privacy Officer; and
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.
21.0 Information Technology Security and PRIVACY TRAINING (MAR 2015)
(a) Applicability. This clause applies to the Contractor, its subcontractors, and Contractor employees (hereafter referred to collectively as “Contractor”). The Contractor shall insert the substance of this clause in all subcontracts.
(b) Security Training Requirements.

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

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

**Accessibility Requirements (Section 508)**

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

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

Section 508 Applicable EIT Accessibility Standards

36 CFR 1194.21 Software Applications and Operating Systems, applies to all EIT software applications and operating systems procured or developed under this work statement including but not limited to GOTS and COTS software. In addition, this standard is to be applied to Web-based applications when needed to fulfill the functional performance criteria. This standard also applies to some Web based applications as described within 36 CFR 1194.22.
36 CFR 1194.22 Web-based Intranet and Internet Information and Applications, applies to all Web-based deliverables, including documentation and reports procured or developed under this work statement. When any Web application uses a dynamic (non-static) interface, embeds custom user control(s), embeds video or multimedia, uses proprietary or technical approaches such as, but not limited to, Flash or Asynchronous Javascript and XML (AJAX) then 1194.21 Software standards also apply to fulfill functional performance criteria.
36 CFR 1194.24 Video and Multimedia Products, applies to all video and multimedia products that are procured or developed under this work statement. Any video or multimedia presentation shall also comply with the software standards (1194.21) when the presentation is through the use of a Web or Software application interface having user controls available.
36 CFR 1194.31 Functional Performance Criteria, applies to all EIT deliverables regardless of delivery method. All EIT deliverable shall use technical standards, regardless of technology, to fulfill the functional performance criteria.
36 CFR 1194.41 Information Documentation and Support, applies to all documents, reports, as well as help and support services. To ensure that documents and reports fulfill the required 1194.31 Functional Performance Criteria, they shall comply with the technical standard associated with Web-based Intranet and Internet Information and Applications at a minimum. In addition, any help or support provided in this work statement that offer telephone support, such as, but not limited to, a help desk shall have the ability to transmit and receive messages using TTY.

Section 508 Applicable Exceptions

Exceptions for this work statement have been determined by DHS and only the exceptions described herein may be applied. Any request for additional exceptions shall be sent to the COTR and determination will be made in accordance with DHS MD 4010.2. DHS has identified the following exceptions that may apply:

36 CFR 1194.3(b) Incidental to Contract, all EIT that is exclusively owned and used by the contractor to fulfill this work statement does not require compliance with Section 508. This exception does not apply to any EIT deliverable, service or item that will be used by any Federal employee(s) or member(s) of the public. This exception only applies to those contractors assigned to fulfill the obligations of this work statement and for the purposes of this requirement, are not considered members of the public.

Section 508 Compliance Requirements

36 CFR 1194.2(b) (COTS/GOTS products), When procuring a product, each agency shall procure products which comply with the provisions in this part when such products are available in the commercial marketplace or when such products are developed in response to a Government solicitation. 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@hq.dhs.gov.

"Personally Identifiable Information (PII)" as used in this clause means any information that permits the identity of an individual to be directly or indirectly inferred, including any other information that is linked or linkable to that individual regardless of whether the individual is a citizen of the United States, legal permanent resident, or a visitor to the United States. Sensitive PII is a subset of PII which requires additional precautions to prevent exposure or compromise. Examples of PII include: 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), Internet protocol addresses, biometric identifiers (e.g., fingerprints), 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 Personally Identifiable Information (Sensitive PII)" as used in this clause is a subset of Personally Identifiable Information, which if lost, compromised or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Complete social security numbers (SSN), alien registration numbers (A-number) and biometric identifiers (such as fingerprint, voiceprint, or iris scan) are considered Sensitive PII even if they are not coupled with additional PII. Additional examples include any groupings of information that contains an individual's name or other unique identifier plus one or more of the following elements:

(1) Driver's license number, passport number, or truncated SSN (such as last 4 digits)
(2) Date of birth (month, day, and year)
(3) Citizenship or immigration status
(4) Financial information such as account numbers or Electronic Funds Transfer Information
(5) Medical Information
(6) System authentication information such as mother's maiden name, account passwords or personal identification numbers (PIN)

Other Personally Identifiable information may be "sensitive" depending on its context, such as a list of employees with less than satisfactory 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 it is not sensitive.

***(b) Systems Access.*** Work to be performed under this contract requires the handling of PII and/or Sensitive PII. The contractor shall provide USCIS access to, and information regarding systems the contractor operates on behalf of USCIS under this contract, when requested by USCIS, as part of its responsibility to ensure compliance with security requirements, and shall otherwise cooperate with USCIS in assuring compliance with such requirements. USCIS access shall include independent validation testing of controls, system penetration testing by USCIS, Federal Information Security Management Act (FISMA) data reviews, and access by agency Inspectors General for its reviews.

***(c) Systems Security.*** In performing its duties related to management, operation, and/or access of systems, owned and or operated by USCIS as well as by the contractor, containing PII and/or Sensitive PII under this contract, the contractor, its employees and subcontractors shall comply with applicable security requirements described in Department of Homeland Security (DHS) Sensitive System Publication 4300A or any superseding publication, and Rules of Behavior.

In addition, use of contractor-owned laptops or other mobile media storage devices to include external hard drives and memory sticks to process or store PII/Sensitive PII is prohibited under this contract unless the Contracting Officer (CO) in coordination with the USCIS Chief

Information Security Officer (CISO) approves. If approval is granted the contractor shall provide written certification that the following minimum requirements are met:
(1) Laptops shall employ full disk encryption using NIST Federal Information Processing Standard (FIPS) 140-2 or successor approved product;
(2) Mobile computing devices use anti-viral software and a host-based firewall mechanism;
(3) When no longer needed, all mobile media and laptop hard drives shall be processed (i.e., sanitized, degaussed, and/or destroyed) in accordance with DHS security requirements set forth in DHS Sensitive System Publication 4300A. The USCIS reserves the right to audit random media for effectiveness of sanitization or degaussing. The contractor shall provide the requested equipment to USCIS no later than 15 days from the date of the request.
(4) The contractor shall maintain an accurate inventory of devices used in the performance of this contract and be made available upon request from USCIS;
(5) All Sensitive PII obtained under this contract shall be removed from contractorowned information technology assets upon termination or expiration of contractor work. Removal must be accomplished in accordance with DHS Sensitive System Publication 4300A, which the Contracting Officer will provide upon request. Certification of data removal will be performed by the contractor's Project Manager and written notification confirming certification will be delivered to the contracting officer within 15 days of termination/expiration of contractor work.
***(d) Data Security.*** Contractor shall limit access to the data covered by this clause to those employees and subcontractors who require the information in order to perform their official duties under this contract. The contractor, contractor employees, and subcontractors must physically secure PII/Sensitive PII when not in use and/or under the control of an authorized individual, and when in transit to prevent unauthorized access or loss. When PII/Sensitive PII is no longer needed or required to be retained under applicable Government records retention policies, it must be destroyed through means that will make the PII/Sensitive PII irretrievable. The contractor shall only use PII/Sensitive PII obtained under this contract for purposes of the contract, and shall not collect or use such information for any other purpose without the prior written approval of the Contracting Officer. At expiration or termination of this contract, the contractor shall turn over all PII/Sensitive PII obtained under the contract that is in its possession to USCIS.
***(e) Breach Response.*** The contractor agrees that in the event of any actual or suspected breach of PII/Sensitive PII (i.e., loss of control, compromise, unauthorized disclosure, access for an unauthorized purpose, or other unauthorized access, whether physical or electronic), it shall immediately, and in no event later than one hour of discovery, report the breach to the Contracting Officer , the Contracting Officer's Representative (COR), and the USCIS Service Desk and complete an Incident Report with the Service Desk Representative. The contractor is responsible for positively verifying that notification is received and acknowledged by at least one of the foregoing Government parties. Email notification shall be used to document all telephonic notifications.
***(f) Personally Identifiable Information Notification Requirement.*** The contractor will have in place procedures and the capability to promptly notify any individual whose PII/Sensitive PII was, or is reasonably believed to have been, breached, as determined appropriate by USCIS. The method and content of any notification by the contractor shall be coordinated with, and subject to the prior approval of USCIS, based upon a risk-based analysis conducted by USCIS in accordance with DHS Privacy incident Handling Guidance and USCIS Privacy Incident

Standard Operating Procedures. Notification shall not proceed unless USCIS has determined that: (1) notification is appropriate; and (2) would not impede a law enforcement investigation or jeopardize national security.

Subject to USCIS analysis of the breach and the terms of its instructions to the contractor regarding any resulting breach notification, a method of notification may include letters to affected individuals sent by first class mail, electronic means, or general public notice, as approved by USCIS. At minimum, a notification should include: (1) a brief description of how the breach occurred; (2) a description of the types of personal information involved in the breach; (3) a statement as to whether the information was encrypted or protected by other means; (4) steps an individual may take to protect themselves; (5) what the agency is doing, if anything, to investigate the breach, to mitigate losses, and to protect against any further breaches; and (6) point of contact information identifying who affected individuals may contact for further information.

The contractor agrees to assist in and comply with PII/Sensitive PII incident remediation and/or mitigation efforts and instructions, including those breaches that are not a result of the contractor or employee actions, but the contractor is an unintentional recipient of privacy data. Actions may include allowing USCIS incident response personnel to have access to computing equipment or storage devices, complying with instructions to remove emails or files from local or network drives, mobile devices (BlackBerry, Smart Phone, iPad, USB thumbdrives, etc…).

In the event that a PII/Sensitive PII breach occurs as a result of the violation of a term of this contract by the contractor or its employees, the contractor shall, as directed by the contracting officer and at no cost to USCIS, take timely action to correct or mitigate the violation, which may include providing notification and/or other identity protection services to affected individuals for a period not to exceed 12 months from discovery of the breach. Should USCIS elect to provide and/or procure notification or identity protection services in response to a breach, the contractor will be responsible for reimbursing USCIS for those expenses. To ensure continuity with existing government identity protection and credit monitoring efforts, the contractor shall use the identity protection service provider specified by USCIS.

***(g) Privacy Training Requirement.*** The performance of this contract has been determined to have the potential of allowing access, by Offeror employees, to Personally Identifiable Information (PII) and/or Sensitive PII, which is protected under the Privacy Act of 1974, as amended at 5 USC §552a. The Offeror is responsible for ensuring all employees who have access to information protected under the Privacy Act complete annual mandatory USCIS Privacy Awareness Training. New Offeror employees shall complete PII training within 30 days of entry on duty. The Offeror shall use the USCIS provided web-based Privacy Training which is available through the USCIS LearningEdge training system http://learningedge.uscis.dhs.gov to satisfy this requirement. Any employees who do not have access to the online LearningEdge training system shall take Privacy training via a USCIS provided DVD. The Offeror shall certify as soon as this training is completed by its employees and annually thereafter on September 30th. The certification of the completion of the training by all employees shall be provided to both the COR and CO; within 60 days of contract award, within 45 days of new employee accession and no later than September 30th for the annual recertification.

***(h) Pass-Through of Security Requirements to Subcontractors.*** The contractor agrees to incorporate the substance of this clause, its terms and requirements, in all subcontracts under this contract, and to require written subcontractor acknowledgement of same. Violation by a subcontractor of any provision set forth in this clause will be attributed to the contractor.

***(i) Ability to Restrict Access to Information***. 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 Personally Identifiable Information (PII), Sensitive PII (SPII), Sensitive But Unclassified (SBU) information and/or classified information.

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

# SECURITY REQUIREMENTS

## FACILITY ACCESS CONTROL

The Contractor will observe all internal building security regulations that apply to any and all buildings concerning this contract. The Contractor will only enter the facility or building with continuous escort service during their work hours and they will depart the facility or building after work hours. When entering and departing the facility or building each contractor must sign in and out as required at the site.

## EMPLOYMENT OF ILLEGAL ALIENS

Subject to existing law, regulations and other provisions of this contract, the Contractor shall not employ illegal or undocumented aliens to work on, or with this contract. The Contractor shall ensure that this provision is expressly incorporated into any and all subcontracts or subordinate agreements issued in support of this contract.