


SOLICITATION/CONTRACT/ORDER FOR COMMERCIAL ITEMS <i>OFFEROR TO COMPLETE BLOCKS 12, 17, 23, 24, & 30</i>				1. REQUISITION NUMBER OIT192108		PAGE OF 1 28						
2. CONTRACT NO. HSHQDC13DE2026			3. AWARD/ EFFECTIVE DATE		4. ORDER NUMBER 70SBUR19F00000607		5. SOLICITATION NUMBER 70SBUR19R00000101					
							6. SOLICITATION ISSUE DATE 09/25/2019					
7. FOR SOLICITATION INFORMATION CALL:		a. NAME MORGAN SKAGGS				b. TELEPHONE NUMBER (No collect calls) 8028724154		8. OFFER DUE DATE/LOCAL TIME				
9. ISSUED BY USCIS Contracting Office Department of Homeland Security 70 Kimball Avenue South Burlington VT 05403			CODE CIS		10. THIS ACQUISITION IS <input checked="" type="checkbox"/> SMALL BUSINESS <input type="checkbox"/> HUBZONE SMALL BUSINESS <input type="checkbox"/> SERVICE-DISABLED VETERAN-OWNED SMALL BUSINESS <input type="checkbox"/> UNRESTRICTED OR <input type="checkbox"/> WOMEN-OWNED SMALL BUSINESS (WOSB) ELIGIBLE UNDER THE WOMEN-OWNED SMALL BUSINESS PROGRAM <input type="checkbox"/> EDWOSB <input type="checkbox"/> 8(A)				13b. RATING 100.00 % FOR: NAICS: SIZE STANDARD:			
11. DELIVERY FOR FOB DESTINATION UNLESS BLOCK IS MARKED <input checked="" type="checkbox"/> SEE SCHEDULE		12. DISCOUNT TERMS Net 30			13a. THIS CONTRACT IS A RATED ORDER UNDER DPAS (15 CFR 700) <input type="checkbox"/>		14. METHOD OF SOLICITATION <input type="checkbox"/> RFQ <input type="checkbox"/> IFB <input checked="" type="checkbox"/> RFP					
15. DELIVER TO Department of Homeland Security US Citizenship & Immigration Svcs Office of Information Technology 111 Massachusetts Ave, NW Suite 5000 Washington DC 20529			CODE HQOIT		16. ADMINISTERED BY USCIS Contracting Office Department of Homeland Security 70 Kimball Avenue South Burlington VT 05403				CODE CIS			
17a. CONTRACTOR/ OFFEROR TECHNICAL AND MANAGEMENT RESOURCES INC PO BOX 1254 LORTON VA 221991254			CODE 0413165190000 FACILITY CODE		18a. PAYMENT WILL BE MADE BY See Invoicing Instructions				CODE WEBVIEW			
TELEPHONE NO.												
<input type="checkbox"/> 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 <input type="checkbox"/> SEE ADDENDUM							
19. ITEM NO.		20. SCHEDULE OF SUPPLIES/SERVICES			21. QUANTITY		22. UNIT		23. UNIT PRICE		24. AMOUNT	
		DUNS Number: 041316519+0000 This is an Enterprise Acquisition Gateway for Leading-Edge Solutions II (EAGLE II) Functional Category 2 (FC2) Small Business Track set-aside firm-fixed price (FFP) task order. All EAGLE II FC2 Small Business track contract HSHQDC-13-D-E2026 terms and conditions shall apply. PSC: D307 AAP Number: 2019048082 Continued ... (Use Reverse and/or Attach Additional Sheets as Necessary)										
25. ACCOUNTING AND APPROPRIATION DATA See schedule								26. TOTAL AWARD AMOUNT (For Govt. Use Only) \$335,743.50				
<input type="checkbox"/> 27a. SOLICITATION INCORPORATES BY REFERENCE FAR 52.212-1, 52.212-4, FAR 52.212-3 AND 52.212-5 ARE ATTACHED. ADDENDA								<input type="checkbox"/> ARE <input type="checkbox"/> ARE NOT ATTACHED.				
<input checked="" type="checkbox"/> 27b. CONTRACT/PURCHASE ORDER INCORPORATES BY REFERENCE FAR 52.212-4. FAR 52.212-5 IS ATTACHED. ADDENDA								<input type="checkbox"/> ARE <input checked="" type="checkbox"/> ARE NOT ATTACHED.				
<input type="checkbox"/> 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.					<input checked="" type="checkbox"/> 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) 							
30b. NAME AND TITLE OF SIGNER (Type or print)			30c. DATE SIGNED		31b. NAME OF CONTRACTING OFFICER (Type or print) HOLLIE L. WALSH			31c. DATE SIGNED 9/30/19				

19. ITEM NO.	20. SCHEDULE OF SUPPLIES/SERVICES	21. QUANTITY	22. UNIT	23. UNIT PRICE	24. AMOUNT
0001	<p>Delivery: 10 Days After Authorization to Work</p> <p>Accounting Info:</p> <p>ITALM00 SMA EX 20-01-00-000</p> <p>23-20-0200-00-00-00-00 GE-25-47-00 000000</p> <p>Oracle Subject Matter Expert Services in accordance with Section 5 of the SOW (FFP)</p> <p>Part II - Terms and Conditions</p> <p>Part III - Attachments</p> <p>Attachment 1: Statement of Work (SOW)</p> <p>Attachment 2: Security Requirements</p> <p>The total amount of award: \$335,743.50. The obligation for this award is shown in box 26.</p>				335,743.50

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. MAILING ADDRESS OF AUTHORIZED GOVERNMENT REPRESENTATIVE			32f. TELEPHONE NUMBER OF AUTHORIZED GOVERNMENT REPRESENTATIVE	
			32g. E-MAIL OF AUTHORIZED GOVERNMENT REPRESENTATIVE	
33. SHIP NUMBER	34. VOUCHER NUMBER	35. AMOUNT VERIFIED CORRECT FOR	36. PAYMENT <input type="checkbox"/> COMPLETE <input type="checkbox"/> PARTIAL <input type="checkbox"/> FINAL	37. CHECK NUMBER
<input type="checkbox"/> PARTIAL <input type="checkbox"/> FINAL				
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 CERTIFYING OFFICER		42b. RECEIVED AT (Location)		
		42c. DATE REC'D (YY/MM/DD)		42d. TOTAL CONTAINERS

PART II – TERMS AND CONDITIONS

ALL EAGLE II FC2 SMALL BUSINESS TERMS AND CONDITIONS SHALL APPLY

FAR CLAUSES BY REFERENCE

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

52.204-13 System for Award Management Maintenance (OCT 2018)

52.204-18 Commercial and Government Entity Code Maintenance (JUL 2016)

52.204-19 Incorporation by Reference of Representations and Certifications (DEC 2014)

52.209-10 Prohibition on Contracting with Inverted Domestic Corporations (NOV 2015)

52.219-28 Post-Award Small Business Program Rerepresentation (JUL 2013)

52.222-44 Fair Labor Standards Act and Service Contract Labor Standards-Price Adjustment (MAY 2014)

52.232-39 Unenforceability of Unauthorized Obligation (JUN 2013)

FAR CLAUSES FULL TEXT

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

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

Covered foreign country means The People's Republic of China.

Covered telecommunications equipment or services means--

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

Critical technology means--

- (1) Defense articles or defense services included on the United States Munitions List set forth in the International Traffic in Arms Regulations under subchapter M of chapter I of title 22, Code of Federal Regulations;
- (2) Items included on the Commerce Control List set forth in Supplement No. 1 to part 774 of the Export Administration Regulations under subchapter C of chapter VII of title 15, Code of Federal Regulations, and controlled--
 - (i) Pursuant to multilateral regimes, including for reasons relating to national security, chemical and biological weapons proliferation, nuclear nonproliferation, or missile technology; or

- (ii) For reasons relating to regional stability or surreptitious listening;
 - (3) Specially designed and prepared nuclear equipment, parts and components, materials, software, and technology covered by part 810 of title 10, Code of Federal Regulations (relating to assistance to foreign atomic energy activities);
 - (4) Nuclear facilities, equipment, and material covered by part 110 of title 10, Code of Federal Regulations (relating to export and import of nuclear equipment and material);
 - (5) Select agents and toxins covered by part 331 of title 7, Code of Federal Regulations, part 121 of title 9 of such Code, or part 73 of title 42 of such Code; or
 - (6) Emerging and foundational technologies controlled pursuant to section 1758 of the Export Control Reform Act of 2018 (50 U.S.C. 4817). Substantial or essential component means any component necessary for the proper function or performance of a piece of equipment, system, or service.
- (b) Prohibition. Section 889(a)(1)(A) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232) prohibits the head of an executive agency on or after August 13, 2019, from procuring or obtaining, or extending or renewing a contract to procure or obtain, any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system. The Contractor is prohibited from providing to the Government any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system, unless an exception at paragraph (c) of this clause applies or the covered telecommunication equipment or services are covered by a waiver described in Federal Acquisition Regulation 4.2104.
- (c) Exceptions. This clause does not prohibit contractors from providing--
- (1) A service that connects to the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements; or
 - (2) Telecommunications equipment that cannot route or redirect user data traffic or permit visibility into any user data or packets that such equipment transmits or otherwise handles.
- (d) Reporting requirement.
- (1) In the event the Contractor identifies covered telecommunications equipment or services used as a substantial or essential component of any system, or as critical technology as part of any system, during contract performance, or the Contractor is notified of such by a subcontractor at any tier or by any other source, the Contractor shall report the information in paragraph (d)(2) of this clause to the Contracting Officer, unless elsewhere in this contract are established procedures for reporting the information; in the case of the Department of Defense, the Contractor shall report to the website at <https://dibnet.dod.mil>. For indefinite delivery contracts, the Contractor shall report to the Contracting Officer for the indefinite delivery contract and the Contracting Officer(s) for any affected order or, in the case of the Department of Defense, identify both the indefinite delivery contract and any affected orders in the report provided at <https://dibnet.dod.mil>.
 - (2) The Contractor shall report the following information pursuant to paragraph (d)(1) of this clause:
 - (i) Within one business day from the date of such identification or notification: The contract number; the order number(s), if applicable; supplier name; supplier unique entity identifier (if known); supplier Commercial and Government Entity (CAGE) code (if known); brand; model number (original equipment manufacturer number, manufacturer part number, or wholesaler number); item description; and any readily available information about mitigation actions undertaken or recommended.

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

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

(End of Clause)

52.219-6 Notice of Total Small Business Set-Aside (NOV 2011)(DEVIATION 2019-01).

(a) *Definition.* *Small business concern*, as used in this clause, means a concern, including its affiliates that is independently owned and operated, not dominant in the field of operation in which it is bidding on Government contracts, and qualified as a small business under the size standards in this solicitation.

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

- (1) Contracts that have been totally set aside or reserved for small business concerns; and
- (2) Orders set aside for small business concerns under multiple-award contracts as described in 8.405-5 and 16.505(b)(2)(i)(F).

(c) *General.*

- (1) Offers are solicited only from small business concerns. Offers received from concerns that are not small business concerns shall be considered nonresponsive and will be rejected.
- (2) Any award resulting from this solicitation will be made to a small business concern.

(d) *Agreement.*

[(1) For a contract at or below the simplified acquisition threshold, a small business concern may provide the end item of any firm. For a contract exceeding the simplified acquisition threshold, a small business concern that provides an end item it did not manufacture, process, or produce, shall—

- (i) Provide an end item that a small business has manufactured, processed, or produced in the United States or its outlying areas;
- (ii) Be primarily engaged in the retail or wholesale trade and normally sell the type of item being supplied; and
- (iii) Take ownership or possession of the item(s) with its personnel, equipment, or facilities in a manner consistent with industry practice; for example, providing storage, transportation, or delivery.

(2) Paragraph (d)(1) of this clause does not apply to construction or service contracts.]

(End of clause)

52.219-14 Limitations on Subcontracting (JAN 2017)(DEVIATION 2019-01)

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

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

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

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

- (1) Contracts that have been set aside or reserved any of the small business concerns identified in 19.000(a)(3);
 - (2) Part or parts of a multiple-award contract that have been set aside for any of the small business concerns identified in 19.000(a)(3);
 - (3) Contracts that have been awarded on a sole-source basis in accordance with subparts 19.8, 19.13, 19.14, and 19.15; and
 - (4) Orders set aside for any of the small business concerns identified in 19.000(a)(3) under multiple-award contracts as described in 8.405-5 and 16.505(b)(2)(i)(F).
- (d) *Independent contractors.* An independent contractor shall be considered a subcontractor.
- (e) *Agreement.* By submission of an offer and execution of a contract, the Offeror/Contractor agrees in performance of the contract in the case of a contract for—
- (1) Services (except construction), it will not pay more than 50 percent of the amount paid by the Government for contract performance to subcontractors that are not similarly situated entities. Any work that a similarly situated entity further subcontracts will count toward the 50 percent subcontract amount that cannot be exceeded;
 - (2) Supplies (other than procurement from a nonmanufacturer of such supplies), it will not pay more than 50 percent of the amount paid by the Government for contract performance, excluding the cost of materials, to subcontractors that are not similarly situated entities. Any work that a similarly situated entity further subcontracts will count toward the 50 percent subcontract amount that cannot be exceeded;
 - (3) General construction, it will not pay more than 85 percent of the amount paid by the Government for contract performance, excluding the cost of materials, to subcontractors that are not similarly situated entities. Any work that a similarly situated entity further subcontracts will count toward the 85 percent subcontract amount that cannot be exceeded; or
 - (4) Construction by special trade contractors, it will not pay more than 75 percent of the amount paid by the Government for contract performance, excluding the cost of materials, to subcontractors that are not similarly situated entities. Any work that a similarly situated entity further subcontracts will count toward the 75 percent subcontract amount that cannot be exceeded.
- (f) A joint venture agrees that, in the performance of the contract, the applicable percentage specified in paragraph (e) of this clause will be performed by the aggregate of the joint venture participants.

(End of clause)

52.252-2 -- Clauses Incorporated by Reference (FEB 1998)

This contract incorporates one or more clauses by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. Also, the full text of a clause may be accessed electronically at this/these address(es):

www.acquisition.gov/browsefar

(End of Clause)

52.252-6 -- Authorized Deviations in Clauses (APR 1984)

(a) The use in this solicitation or contract of any Federal Acquisition Regulation (48 CFR Chapter 1) clause with an authorized deviation is indicated by the addition of “(DEVIATION)” after the date of the clause.

(b) The use in this solicitation or contract of any Homeland Security Acquisition Regulation (48 CFR Chapter 30) clause with an authorized deviation is indicated by the addition of “(DEVIATION)” after the date of the clause.

(End of Clause)

HSAR CLAUSES BY REFERENCE

3052.204-71 Contractor employee access (SEP 2012)

3052.205-70 Advertisements, Publicizing Awards, and Releases (SEP 2012)

3052.215-70 Key personnel or facilities (DEC 2003)

Fill-in: The Key Personnel or Facilities under this Contract: One (1) Subject Matter Expert, one (1) Project Manager.

3052.222-70 Strikes or picketing affecting timely completion of the contract work (DEC 2003)

3052.222-71 Strikes or picketing affecting access to a DHS facility (DEC 2003)

HSAR CLAUSES FULL TEXT

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.

(ci) *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.

(cii) 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.

(ciii) *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.

(civ) 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)

<p>USCIS LOCAL CLAUSES</p>

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 or any disagreements with the Contractor's redactions before public posting of the contract or order in a public FOIA reading room.

DHS ENTERPRISE ARCHITECTURE COMPLIANCE

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

- a) All developed solutions and requirements shall be compliant with the 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.

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

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

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

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

PII is a subset of sensitive information. Examples of PII include, but are not limited to: name, date of birth, mailing address, telephone number, Social Security number (SSN), email address, zip code,

account numbers, certificate/license numbers, vehicle identifiers including license plates, uniform resource locators (URLs), static Internet protocol addresses, biometric identifiers such as fingerprint, voiceprint, iris scan, photographic facial images, or any other unique identifying number or characteristic, and any information where it is reasonably foreseeable that the information will be linked with other information to identify the individual.

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

- (1) Protected Critical Infrastructure Information (PCII) as set out in the Critical Infrastructure Information Act of 2002 (Title II, Subtitle B, of the Homeland Security Act, Public Law 107-296, 196 Stat. 2135), as amended, the implementing regulations thereto (Title 6, Code of Federal Regulations, Part 29) as amended, the applicable PCII Procedures Manual, as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the PCII Program Manager or his/her designee);
- (2) Sensitive Security Information (SSI), as defined in Title 49, Code of Federal Regulations, Part 1520, as amended, “Policies and Procedures of Safeguarding and Control of SSI,” as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the Assistant Secretary for the Transportation Security Administration or his/her designee);
- (3) Information designated as “For Official Use Only,” which is unclassified information of a sensitive nature and the unauthorized disclosure of which could adversely impact a person’s privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national or homeland security interest; and
- (4) Any information that is designated “sensitive” or subject to other controls, safeguards or protections in accordance with subsequently adopted homeland security information handling procedures.

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

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

- (1) Truncated SSN (such as last 4 digits)
- (2) Date of birth (month, day, and year)
- (3) Citizenship or immigration status
- (4) Ethnic or religious affiliation
- (5) Sexual orientation

- (6) Criminal History
- (7) Medical Information
- (8) System authentication information such as mother's maiden name, account passwords or personal identification numbers (PIN)

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

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

- (1) DHS Management Directive 11042.1 Safeguarding Sensitive But Unclassified (for Official Use Only) Information
- (2) DHS Sensitive Systems Policy Directive 4300A
- (3) DHS 4300A Sensitive Systems Handbook and Attachments
- (4) DHS Security Authorization Process Guide
- (5) DHS Handbook for Safeguarding Sensitive Personally Identifiable Information
- (6) DHS Instruction Handbook 121-01-007 Department of Homeland Security Personnel Suitability and Security Program
- (7) DHS Information Security Performance Plan (current fiscal year)
- (8) DHS Privacy Incident Handling Guidance
- (9) Federal Information Processing Standard (FIPS) 140-2 Security Requirements for Cryptographic Modules accessible at <http://csrc.nist.gov/groups/STM/cmvp/standards.html>
- (10) National Institute of Standards and Technology (NIST) Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations accessible at <http://csrc.nist.gov/publications/PubsSPs.html>
- (11) NIST Special Publication 800-88 Guidelines for Media Sanitization accessible at <http://csrc.nist.gov/publications/PubsSPs.html>

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

- (1) Department of Homeland Security (DHS) policies and procedures on Contractor personnel security requirements are set forth in various Management Directives (MDs), Directives, and Instructions. *MD 11042.1, Safeguarding Sensitive But Unclassified (For Official Use Only) Information* describes how Contractors must handle sensitive but unclassified information. DHS uses the term "FOR OFFICIAL USE ONLY" to identify sensitive but unclassified information that is not otherwise categorized by statute or regulation. Examples of sensitive information that are categorized by statute or regulation are PCII, SSI, etc. The *DHS Sensitive Systems Policy Directive 4300A* and the *DHS 4300A Sensitive Systems Handbook* provide the policies and procedures on security for Information Technology (IT) resources. The *DHS Handbook for Safeguarding Sensitive Personally Identifiable Information* provides guidelines to help safeguard SPII in both paper and electronic form. *DHS Instruction Handbook 121-01-007 Department of Homeland Security Personnel Suitability and Security Program* establishes procedures, program responsibilities, minimum standards, and reporting protocols for the DHS Personnel Suitability and Security Program.
- (2) The Contractor shall not use or redistribute any sensitive information processed, stored, and/or transmitted by the Contractor except as specified in the contract.
- (3) All Contractor employees with access to sensitive information shall execute *DHS Form 11000-6, Department of Homeland Security Non-Disclosure Agreement (NDA)*, as a condition of access to such information. The Contractor shall maintain signed copies of the NDA for all

employees as a record of compliance. The Contractor shall provide copies of the signed NDA to the Contracting Officer's Representative (COR) no later than two (2) days after execution of the form.

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

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

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

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

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

(iii) Support the completion of the Privacy Threshold Analysis (PTA) as needed. As part of the SA process, the Contractor may be required to support the Government in the completion of the PTA. The requirement to complete a PTA is triggered by the creation, use, modification, upgrade, or disposition of a Contractor IT system that will store, maintain and use PII, and must be renewed at least every three (3) years. Upon review of the PTA, the DHS Privacy Office determines whether a Privacy Impact

Assessment (PIA) and/or Privacy Act System of Records Notice (SORN), or modifications thereto, are required. The Contractor shall provide all support necessary to assist the Department in completing the PIA in a timely manner and shall ensure that project management plans and schedules include time for the completion of the PTA, PIA, and SORN (to the extent required) as milestones. Support in this context includes responding timely to requests for information from the Government about the use, access, storage, and maintenance of PII on the Contractor's system, and providing timely review of relevant compliance documents for factual accuracy. Information on the DHS privacy compliance process, including PTAs, PIAs, and SORNs, is accessible at <http://www.dhs.gov/privacy-compliance>.

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

(1) Updating the SA documentation in the DHS automated information assurance tool for acceptance by the Headquarters or Component CIO, or designee, at least 90 days before the ATO expiration date for review and verification of security controls; or (2) Submitting an updated SA package directly to the COR for approval by the Headquarters or Component CIO, or designee, at least 90 days before the ATO expiration date for review and verification of security controls. The 90 day review process is independent of the system production date and therefore it is important that the Contractor build the review into project schedules. The reviews may include onsite visits that involve physical or logical inspection of the Contractor environment to ensure controls are in place.

(3) *Security Review*. The Government may elect to conduct random periodic reviews to ensure that the security requirements contained in this contract are being implemented and enforced. The Contractor shall afford DHS, the Office of the Inspector General, and other Government organizations access to the Contractor's facilities, installations, operations, documentation, databases and personnel used in the performance of this contract. The Contractor shall, through the Contracting Officer and COR, contact the Headquarters or Component CIO, or designee, to coordinate and participate in review and inspection activity by Government organizations external to the DHS. Access shall be provided, to the extent necessary as determined by the

Government, for the Government to carry out a program of inspection, investigation, and audit to safeguard against threats and hazards to the integrity, availability and confidentiality of Government data or the function of computer systems used in performance of this contract and to preserve evidence of computer crime.

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

(5) *Revocation of ATO*. In the event of a sensitive information incident, the Government may suspend or revoke an existing ATO (either in part or in whole). If an ATO is suspended or revoked in accordance with this provision, the Contracting Officer may direct the Contractor

to take additional security measures to secure sensitive information. These measures may include restricting access to sensitive information on the Contractor IT system under this contract. Restricting access may include disconnecting the system processing, storing, or transmitting the sensitive information from the Internet or other networks or applying additional security controls.

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

(f) *Sensitive Information Incident Reporting Requirements.*

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

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

- (i) Data Universal Numbering System (DUNS);
- (ii) Contract numbers affected unless all contracts by the company are affected;
- (iii) Facility CAGE code if the location of the event is different than the prime contractor location;
- (iv) Point of contact (POC) if different than the POC recorded in the System for Award Management (address, position, telephone, email);
- (v) Contracting Officer POC (address, telephone, email); (vi) Contract clearance level;
- (vii) Name of subcontractor and CAGE code if this was an incident on a subcontractor network;
- (viii) Government programs, platforms or systems involved; (ix) Location(s) of incident;
- (x) Date and time the incident was discovered;

- (xi) Server names where sensitive information resided at the time of the incident, both at the Contractor and subcontractor level;
- (xii) Description of the Government PII and/or SPII contained within the system;
- (xiii) Number of people potentially affected and the estimate or actual number of records exposed and/or contained within the system; and
- (xiv) Any additional information relevant to the incident.

(g) Sensitive Information Incident Response Requirements.

- (1) All determinations related to sensitive information incidents, including response activities, notifications to affected individuals and/or Federal agencies, and related services (e.g., credit monitoring) will be made in writing by the Contracting Officer in consultation with the Headquarters or Component CIO and Headquarters or Component Privacy Officer.
- (2) The Contractor shall provide full access and cooperation for all activities determined by the Government to be required to ensure an effective incident response, including providing all requested images, log files, and event information to facilitate rapid resolution of sensitive information incidents.
- (3) Incident response activities determined to be required by the Government may include, but are not limited to, the following:
 - (i) Inspections,
 - (ii) Investigations,
 - (iii) Forensic reviews, and
 - (iv) Data analyses and processing.
- (4) The Government, at its sole discretion, may obtain the assistance from other Federal agencies and/or third-party firms to aid in incident response activities.

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

- (1) The Contractor shall have in place procedures and the capability to notify any individual whose PII resided in the Contractor IT system at the time of the sensitive information incident not later than 5 business days after being directed to notify individuals, unless otherwise approved by the Contracting Officer. The method and content of any notification by the Contractor shall be coordinated with, and subject to prior written approval by the Contracting Officer, in consultation with the Headquarters or Component Privacy Officer, utilizing the *DHS Privacy Incident Handling Guidance*. The Contractor shall not proceed with notification unless the Contracting Officer, in consultation with the Headquarters or Component Privacy Officer, has determined in writing that notification is appropriate.
- (2) Subject to Government analysis of the incident and the terms of its instructions to the Contractor regarding any resulting notification, the notification method may consist of letters to affected individuals sent by first class mail, electronic means, or general public notice, as approved by the Government. Notification may require the Contractor's use of address verification and/or address location services. At a minimum, the notification shall include:
 - (i) A brief description of the incident;
 - (ii) A description of the types of PII and SPII involved;
 - (iii) A statement as to whether the PII or SPII was encrypted or protected by other means;
 - (iv) Steps individuals may take to protect themselves;
 - (v) What the Contractor and/or the Government are doing to investigate the incident, to mitigate the incident, and to protect against any future incidents; and
 - (vi) Information identifying who individuals may contact for additional information.

(i) Credit Monitoring Requirements. In the event that a sensitive information incident involves

PII or SPII, the Contractor may be required to, as directed by the Contracting Officer:

- (1) Provide notification to affected individuals as described above; and/or
 - (2) Provide credit monitoring services to individuals whose data was under the control of the Contractor or resided in the Contractor IT system at the time of the sensitive information incident for a period beginning the date of the incident and extending not less than 18 months from the date the individual is notified. Credit monitoring services shall be provided from a company with which the Contractor has no affiliation. At a minimum, credit monitoring services shall include:
 - (i) Triple credit bureau monitoring;
 - (ii) Daily customer service;
 - (iii) Alerts provided to the individual for changes and fraud; and
 - (iv) Assistance to the individual with enrollment in the services and the use of fraud alerts; and/or
 - (3) Establish a dedicated call center. Call center services shall include:
 - (i) A dedicated telephone number to contact customer service within a fixed period;
 - (ii) Information necessary for registrants/enrollees to access credit reports and credit scores;
 - (iii) Weekly reports on call center volume, issue escalation (i.e., those calls that cannot be handled by call center staff and must be resolved by call center management or DHS, as appropriate), and other key metrics;
 - (iv) Escalation of calls that cannot be handled by call center staff to call center management or DHS, as appropriate;
 - (v) Customized FAQs, approved in writing by the Contracting Officer in coordination with the Headquarters or Component Chief Privacy Officer; and
 - (vi) Information for registrants to contact customer service representatives and fraud resolution representatives for credit monitoring assistance.
- (j) *Certification of Sanitization of Government and Government-Activity-Related Files and Information.* As part of contract closeout, the Contractor shall submit the certification to the COR and the Contracting Officer following the template provided in *NIST Special Publication 800-88 Guidelines for Media Sanitization.*
- (End of clause)

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

(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-contractor>

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

(End of clause)

AUTHORIZATION TO WORK (ATW)

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

(b) The contractor is responsible for submitting packages from employees who will receive favorable entry-on-duty (EOD) decisions and suitability determinations, and for submitting them in a timely manner. A government decision to not grant a favorable EOD decision or suitability determination, or to later withdraw or terminate such decision or termination, shall not excuse the contractor from performance of obligations under this task order.

(c) The contractor may submit background investigation packages immediately following task order award.

- (d) This task order does not provide for direct payment to the contractor for EOD efforts. Work for which direct payment is not provided is a subsidiary obligation of the contractor.
- (e) The Government intends for performance to begin no later than 60 days following task order award (allowing up to 60 days for EOD period). All key personnel must have received a favorable EOD prior to issuance of an ATW.
- (f) The contracting officer will issue an ATW at least one day before performance is to begin. The ATW will be done via modification to set the period of performance for the task order.

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 using the "To" line in the e-mail address to USCISInvoice.Consolidation@ice.dhs.gov with each email conforming to a size limit of 500 KB.

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

**USCIS Invoice Consolidation
PO Box 1000
Williston, VT 05495**

STATEMENT OF WORK

1. Title of Project

License Optimization for Oracle: Oracle Database Consolidation Analysis Project

2. Period of Performance

A. The period of performance is for [REDACTED]. The anticipated start of performance is 60 days from award to account for the Entrance on Duty (EOD) Process.

3. Place of Performance

Contractor staff will work at the contractor site or the Office of Information Technology (OIT), located at 111 Massachusetts Avenue, NW, Washington, DC 20529, or upon approved telework.

4. Project Background

A. United States Citizenship and Immigration Services (USCIS) Office of Information Technology (OIT) Applied Technology Division (ATD) Strategic Vendor Management (SVM) has a requirement for license optimization on premise and cloud deployments, and requires the following:

1. Current and Future Architectural Strategy and Consolidation Roadmap for OIT's Oracle Database
2. Data Warehouse Performance Evaluation
3. License Optimization Strategy

This isn't to preclude further compliance analysis, cost optimization, and future license strategy for the products in use at USCIS. This requirement is critical to the functioning, optimizations, cost reduction of the USCIS Oracle applications and platforms within the USCIS infrastructure.

5. Requirement

5.1 Description

A. USCIS OIT has previously invested in Oracle software and hardware, which is currently being utilized. USCIS requires an Oracle Database Enterprise Architectural Optimization Plan and Analysis Report. Services in the agreement will document three phases:

1. Oracle License Assessment and Roadmap
 - a. Perform detailed system analysis and evaluate technical challenges
 - i. Identify technical initiatives within USCIS. For example, major hardware refresh, datacenter build-outs, DR expansions, and business goals.
 - ii. Define AWR statistics retention period for workload assessment and collect statistics based on AWR snapshots

- iii. Provide scripts that extract systems configuration, resource utilization data points for all Oracle databases
 - iv. Gather Flexera FlexNet Manager Oracle report, SunFlower Report and contract awards inventory
 - v. Perform detailed analysis of system resource utilization outputs based on defined workload window to include CPU utilization, IO utilization (OPS/throughput), Memory and Network utilization
 - vi. Identify the technical challenges facing USCIS, such as Availability, Security, Capacity, and Maintenance
 - vii. Identify license over deployments and strategy to mitigate against such actions
 - viii. Roadmap Program Oracle needs over the next 3 years
- b. Database and Infrastructure Target Architecture
 - i. Discuss with stakeholders best practices for Oracle deployments and the different options available to USCIS for enterprise hardware refresh, datacenter build-outs, DR expansions, and business goals
 - ii. Provide Oracle Architecture Consolidation Expertise to different USCIS Programs
 - iii.
 - iv. Perform cost-benefit analysis of different infrastructure and database consolidation options for USCIS, considering Oracle License and Hardware costs
 - v. Validate proposed Oracle licenses with stakeholders
 - vi. Define implementation roadmap for database consolidation strategy
 - vii. Produce business case for consolidated database architecture
- 2. Application Project Data Performance Evaluation
 - a. Discussions with Program and team to understand the project application, business drivers, and technical challenges
 - b.
 - c. Identify system resource utilization and capacity based on defined workload window
 - d. ROI Analysis of multiple solutions for project to find most cost-effective strategy for USCIS
- 3. Oracle License Optimization
 - a. Oracle Negotiations & Communication Strategies
 - i. Give advice and cost optimization strategies for any new Oracle purchases
 - ii. Participate in on-going maintenance/new purchase discussions with Oracle and/or Mythics

- iii. Perform ROI analysis of maintenance scenarios and determine most cost-effective maintenance strategies for USCIS
- b. USCIS Program Mapping to Oracle CSIs
 - i. Map Oracle CSI ownership to USCIS Programs including appropriated and non-appropriated funding programs
 - ii. Remove Oracle accounts not used within the last 45 days and email accounts other than the uscis.dhs.gov domain
 - iii. Assign CSI numbers to the associated server(s)
 - iv. Identify unused licenses and reallocate license to programs in need
 - v. Create go forward strategies of USCIS Programs ownership over identified CSIs and managing compliance
- c. Provide Oracle License Expertise
 - i. Participate in internal meetings and discussions around Oracle Licensing
 - ii. Provide Oracle Best Practice recommendations for cost-efficient license deployments of Oracle
 - iii. Perform ROI analysis of different Oracle licensing scenarios as new projects and infrastructure changes arise

B. Key Personnel

- 1. An Oracle licensing Subject Matter Expert (SME) with Oracle License, Database, and product knowledge experience for both on premise and cloud environments. Oracle Database and an Oracle License certification is preferred, but can be substituted with past experience. A Project Manager (PM) who is responsible for the Project schedule, scope, and budget baselines.

5.2 Deliverables

A. Oracle License Optimization Plan

Contractor will deliver an Oracle License Optimization Plan via hard copy and electronically using PDF, Word, Excel, Visio or other acceptable Microsoft products, at the mid-term and the end of the task order term to SVM. A draft is due 30 prior to the end date of the task order. The government will provide feedback within 5 business days. The final report is due on the last day of the task order period of performance. The deliverable will contain the following:

- 1. OIT's Oracle License Strategy Roadmap
 - a.
 - i. Detailed summary of Current Infrastructure

- Assessment, which includes detailed System Utilization information for every USCIS database instance
 - ii. Detailed spreadsheets with Min/Max/Average CPU/IOPS/MBs and current Memory allocation for each USCIS database mapped to host and best optimal state for Databases for next 3 years
 - iii. Business drivers for Oracle license optimization
 - iv. Technical challenges facing USCIS for optimization
 - v. Oracle license management Best Practices
 - vi. Hardware and Software Recommendations for Oracle Database Consolidation
- b. License Evaluation
 - i. Architecture Diagrams and System details of current project's state
 - ii. Summary of current Technical Challenges
 - iii. System resource utilization charts of Data Warehouse database
 - iv. Recommendations to improve performance and agility for the project Data Warehouse
 - v. Cost-Benefit Analysis of the project with recommended future strategies
 - vi. Oracle License Optimization Strategy
 - vii. Oracle CSI Mapping to identified USCIS Programs before and after states including server configurations and cloud instances
 - viii. Recommendations and go-forward strategies to help USCIS Programs maintain ownership of CSIs, including use of Oracle's portal and use of Flexera Flexenet Manager
 - ix. Oracle maintenance recommendations to better utilize existing licenses and/or remove maintenance to reduce costs
 - x. Best Practice Oracle communication strategies for USCIS
 - xi. Cost-benefit analysis of different licensing scenarios for new projects or infrastructure changes
- 2. Quality Control Plan
 - a. Evaluate procedures used within Agency including stakeholders, vendors, tools, and delivery and tracking of products
 - b. Process control of cloud deployment, monitoring, and tracking.
 - c.
 - d. Issues List
 - i. Report detailing issues preventing the project from proceeding.

- e. Documenting license over and under use cases
- f. Include stakeholder, vendors, length of time, root cause, possible issues and alternate solutions
- 3. Transition Plan
 - a. Document best practices for server configuration to reduce resources, bandwidth, and improper software deployment.
 - b. Record processes to accelerate performance, consolidate environments and repurpose software

5.3 Delivery Table

Subject	Frequency	Section in SOW
Project Plan and Schedule	Within 30 days of task order Notice to Proceed (NTP)	5.
Project Status Reports <ul style="list-style-type: none"> • including all current Work stream status 	Second business day of every month after NTP	5.2 A.1.a 5.2 A.1.b
Oracle Database Optimization Plan <ul style="list-style-type: none"> • Project Plan <ul style="list-style-type: none"> ○ Architectural License Strategy Roadmap ○ Application Performance Evaluation • Quality Control Plan • Transition Plan 	Draft report 30 prior to end of task order Final report: on last day of task order period of performance.	5.2 A
Issues List	Every Tuesday after NTP, and also delivered with Quality Control Plan.	5.2 A.2.e
Power Point Presentation <ul style="list-style-type: none"> • Delivered at post-award conference 	NLT 5 business days after task order award at USCIS OIT HQ.	

6. Specific Tasks

A. The Contractor shall:

1. Provide a single Point of Contact (POC) for management of this order as well as the conduit when needed to work with the software vendor.
2. Any access that the contractor may require to a USCIS facility or system will need authorized USCIS approval. Vendor shall take necessary training to obtain access to USCIS data and facilities.

7. Task Order

A. This is a Firm Fixed Price task order

- B. At no time shall the Contractor make any substitutions for the service support as awarded without prior authorization from the Task Order Contracting Officer (TO CO).
- C. The Contractor shall not accept telephonic orders or modifications, nor any written orders or modifications which are not signed by the TO CO.

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

**Attachment 2
SECURITY REQUIREMENTS**

GENERAL

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

SUITABILITY DETERMINATION

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

BACKGROUND INVESTIGATIONS

Contractor employees (to include applicants, temporaries, part-time and replacement employees) under the contract, needing access to sensitive but unclassified information shall undergo a position sensitivity analysis based on the duties each individual will perform on the contract as outlined in the DHS Form 11000-25, Contractor Fitness/Security Screening Request Form and the USCIS Continuation Page to the DHS Form 11000-25. The results of the position sensitivity analysis shall identify the appropriate background investigation to be conducted. All background investigations will be processed through OSI PSD.

To the extent the DHS Form 11000-25 and the USCIS Continuation Page to the DHS Form 11000-25 reveals that the Contractor will not require access to sensitive but unclassified information or access to USCIS IT systems, OSI PSD may determine that preliminary security screening and or a complete background investigation is not required for performance on this contract.

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

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

26

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. DHS Form 11000-25 "Contractor Fitness/Security Screening Request Form"
5. USCIS Continuation Page to DHS Form 11000-25
6. OF 306, Declaration for Federal Employment (approved use for Federal Contract Employment)
7. Foreign National Relatives or Associates Statement

EMPLOYMENT ELIGIBILITY

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

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

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

CONTINUED ELIGIBILITY

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

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

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

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

- **USCIS Security Awareness Training** (required within 30 days of entry on duty for new contractors, and annually thereafter)
- **USCIS Integrity Training** (Annually)
- **DHS Insider Threat Training** (Annually)
- **DHS Continuity of Operations Awareness Training** (one-time training for contractors identified as providing an essential service)
- **Unauthorized Disclosure Training** (one time training for contractors who require access to USCIS information regardless if performance occurs within USCIS facilities or at a company owned and operated facility)
- **USCIS Fire Prevention and Safety Training** (one-time training for contractors working within USCIS facilities; contractor companies may substitute their own training)
- **Computer Security Awareness Training** (if contractor requires access to USCIS IT systems, training must be completed within 60 days of entry on duty for new contractors, and annually thereafter)

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

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

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 outso that it is visible at all times while in a USCIS facility
 - Keep their PIV card current
 - Properly store the PIV card while not in use to prevent against loss or theft
- <http://ecn.uscis.dhs.gov/team/mgmt/Offices/osi/FSD/HSPD12/SIR/default.aspx>

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

SECURITY MANAGEMENT

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

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

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