U.S. Department of
Homeland Security

**United States
Coast Guard**

Commanding Officer
U.S. Coast Guard
Operations Systems Center

408 Coast Guard Drive
Kearneysville, WV 25430
Staff Symbol: CO
Phone: (304) 264-2550

4200
**April 18, 2019**

To: GSA Contractor

Subject: Request for Quotation (RFQ) 70Z0G319QPBZ02900 (GSA RFQ 1361549) for Workforce Management Tools

The United States Coast Guard (USCG) is issuing this competitive RFQ to solicit selected General Services Administration (GSA), Federal Supply IT Schedule (General Purpose Communication Information Technology Equipment, Software, and Services) contract holders for the purpose of entering into a Blanket Purchase Agreement (BPA) for workforce management software as a service to the United States Coast Guard (USCG). This RFQ does not commit the Government to pay for the preparation and submission of a quotation.

The BPA competition will be conducted pursuant to FAR Subpart 8.4, full and open under IT Schedule 70 SIN 132-51 NAICS 518210. FAR Parts 13, 14 and 15 are not applicable to this RFQ. Offerors are solicited only from IT Schedule 70 SIN 132-51 contract holders.

It is the Government's intent to award a single BPA to the responsible Offeror whose quote, in conforming to the RFQ, provides the overall best value to the Government considering technical and business evaluation factors. For evaluation purposes, and with the intent to award as a call, the AUXDATA Modernization Statement of Work (Attachment 6) is also provided. All calls will be issued Firm-Fixed Price.

A three phase multi-step down select strategy will be used for this procurement. Interested firms are required to submit one Phase I Prior Experience Submission. Failure to participate in Phase I of the solicitation precludes further consideration of an Offeror. After evaluation, Offerors who are rated most highly will be advised to proceed to Phase II of the proposal submission process. Offerors who were not among the most highly rated will be advised that they are unlikely to be viable competitors, along with the general basis for the Government's advisory recommendation. The intent of this advisory notice is to minimize development and other costs for those Offerors with little to no chance of receiving an award. Offerors should note that factors evaluated in Phase I are more important than factors evaluated in Phases II and III. The Government's advice will be a recommendation only, and those Offerors who are advised not to proceed may elect to continue their participation in the procurement.

Offerors participating in Phase II shall provide a Technical demonstration and Oral Presentation. After evaluation, Offerors who are rated most highly will be advised to proceed to Phase III of the proposal

submission process. Offerors who were not among the most highly rated will be advised that they are unlikely to be viable competitors, along with the general basis for the Government's advisory recommendation. The intent of this advisory notice is to minimize development and other costs for those Offerors with little to no chance of receiving an award. Offerors should note that factors evaluated in Phase II are more important than factors evaluated in Phase III. The Government's advice will be a recommendation only, and those Offerors who are advised not to proceed may elect to continue their participation in the procurement.

Offerors participating in Phase III of the evaluation shall provide a Schedule and Price submission.

Any quotation that is non-compliant with any requested submission requirements of this RFQ may immediately be removed from further consideration.

Thank you for your consideration of this request.

Sincerely,

Brenda E. Oberholzer
Contracting Officer

Attachment (1) BPA Statement of Work
Attachment (2) BPA Provisions and Clauses
Attachment (3) BPA Pricing Matrix
Attachment (4) Special Contracting Requirements
Attachment (5) Instructions and Evaluation for Award
Attachment (6) AUXDATA Call Statement of Work

# STATEMENT OF WORK
# FOR
# WORKFORCE MANAGEMENT TOOLS
# U.S. COAST GUARD
# COMMAND, CONTROL, COMMUNICATIONS, COMPUTER
# AND
# INFORMATION TECHNOLOGY SERVICE CENTER

## 1.0 GENERAL

### 1.1 BACKGROUND

The Government has multiple known and unknown future needs to modernize its Workforce Management (WFM) and Customer Relations Management (CRM) tools that are either near or at their end of life. This includes the Recruiting Analysis and Tracking System (RATS) that supports the USCG Recruiters, the USCG Learning Management System (LMS), the USCG Training Management Tool (TMT) which support all active duty, reservists, and Coast Guard Civilians, the AUXDATA system which is the sole system for supporting the Coast Guards 26,000 + members, and various other CRM systems. It is the USCG's objective to obtain a CRM tool, provided as a software as a service, that can be adapted to meet the needs of these related tools and systems, and enable the different functional areas of the USCG to take advantage of the solution chosen for the USCG AUXDATA.

### 1.2 SCOPE

The Government requires software managed service that can be adapted to meet the needs of various human resource units throughout the USCG. The tool will be expected to handle training and learning management, recruiting and workforce development, and most immediately, USCG Auxiliarist Management. Specific functions needed for each will be detailed within the individual calls.

**1.3 REQUIREMENTS:** The Contractor shall provide, implement, and support a Commercial-off-the-shelf (COTS) software tool hosted in a cloud environment to replace USCG systems specified in individual calls. The functional and non-functional requirements for each system will be identified in the individual calls. For each system that is modernized there will be an implementation phase followed by a transition phase where the contractor will be required to transition all data, current users/accounts, and train all end users on the new system. Finally the Contractor shall provide regular maintenance and continued support. The software should, at a minimum, be configurable to do the following:

- Provide a means of access for members and staff.
- Provide a means to manage all members of the USCG and Auxiliary.
- Provide a means to define an organization structure
- Provide a means to establish recruiting targets and goals
- Provide a means to manage recruiting leads
- Provide a means to manage Organizational Units.
- Provide a means to track activities of the USCG.

- Provide a means to track resources of the USCG.
- Provide a means to produce reports on all USCG functions.
- Provide a means to produce reports on USCG functions.
- Provide a means to manage training of the USCG and Auxiliary
- Provide a means to complete training for members of the USCG
- Provide a means to manage security clearances
- Provide a means to process patrol orders
- Provide a means to process training requests
- Provide a means to create various workflows
- Provide a means to communicate to the learning audience
- Provide a means to manage learning content
- Provide a means to query and display specific data
- Provide a means to manage instructor-led course sessions
- Provide a means to manage, execute, and report electronic testing
- Provide a means to manage synchronous and asynchronous e-learning
- Provides a means to manage user roles and system functions

## 1.4 CONTRACTOR PERSONNEL.

The Contractor shall provide contracting support to deliver a fully maintained solution in accordance with the requirements in this SOW and applicable Federal and Agency regulations.

**1.4.1 Key personnel:** The key personnel of this contract are considered to be essential to the work the Contractor agrees to perform hereunder. Prior to diverting the key personnel to other programs, the Contractor shall notify the Contracting Officer's Representative (COR) and the Contracting Officer no less than 15 days in advance and shall submit justification, including proposed substitutions or replacements, in sufficient detail to permit the Contracting Officer to evaluate the impact on the work the Contractor is obligated to perform hereunder. The Contractor shall not replace any of the key personnel without the written consent of the Contracting Officer.

**1.4.1.1 BPA Program Manager (Key Personnel).** The Contractor shall provide a Program Manager who shall be responsible for all contractor work performed under this contract.

**Description of Work:** The Program Manager shall be a single point of contact for the Contracting Officer and the Contracting Officer's Representative (COR). It is anticipated that the Program Manager shall be one of the senior level employees provided by the Contractor for the work effort. The Program Manager shall be responsible for ensuring conformity to contractual obligations, establishing and maintaining master plans and schedules. The Program Manager shall perform day-to-day management of overall contract support operations.

**Experience Requirements**: Shall have a minimum of six (6) years of general IT Project Management experience.

**1.4.2 Qualified Personnel**. For each BPA call, the Contractor shall provide capable and qualified personnel to perform all requirements and tasks specified in this contract. Contractor employees supporting calls shall be able to read, write, speak and understand English fluently, and shall be United States citizens per HSAR 3052.204-71 Alt I.

**1.4.3 Employee Identification.** Contractor employees visiting USCG and other Government facilities shall wear an identification badge that, at minimum, displays the Contractor's name, the employee's photo, name, clearance-level and badge expiration date. Visiting Contractor employees shall comply with all USCG and Government escort rules and requirements. All Contractor employees shall identify themselves as Contractors when their status is not readily apparent and display all identification and visitor badges in plain view above the waist at all times. Contractor employees working on-site at Government facilities shall be identified as contractors on email, at their desks, at meetings, on phone calls, and badges.

**1.4.4 Employee Conduct.** The Contractor's employees shall observe and comply with all applicable regulations, policies and procedures (e.g., fire, safety, sanitation, environmental protection, security, flag officer courtesy, "off limits" areas, wearing of parts of military uniforms, and possession of firearms). The Contractor shall ensure that all contractor employees present a professional appearance at all times, and their conduct does not reflect discredit on the United States, the Department of Homeland Security or the USCG.

The Program Manager shall ensure Contractor employees understand and abide by USCG-established rules, regulations and policies concerning safety and security.

**1.4.5 Removing an Employee for Misconduct or Security Reasons**. The Government at its sole discretion may direct the Contractor to remove any contractor employee from USCG facilities for misconduct or security reasons. Such removal does not relieve the Contractor of the responsibility to provide sufficient qualified staff for adequate and timely service. The Government will provide the Contractor with a written rationale for the removal of the employee through the USCG Contracting Officer.

**1.4.6 Conflict of Interest.** The Contractor shall not employ any person who is an employee of the United States Government if that employee could, or would appear to cause a conflict of interest. If at any time a conflict of interest arises, the Contractor shall inform the Government and also provide a mitigation plan.

**1.5 SPECIAL REQUIREMENTS AND SECURITY.** The Contractor shall adhere to the information systems security (ISS) policies, plans, and procedures administered by the USCG and DHS. The Contractor shall maintain the highest degree of security trust when accessing USCG's resources, networks and, systems. Contractor does not require access to classified information under this contract but will be required to handle Sensitive but Unclassified (SBU) and For Official Use Only (FOUO).

Further requirements are detailed in Section H: Special Contract Requirements.

**1.6 DEPARTMENT OF DEFENSE TRUSTED ASSOCIATE SPONSORSHIP SYSTEM (TASS) AND COMMON ACCESS CARDS:** All Contractor employees working for the USCG shall utilize the Department of Defense (DoD) Trusted Associate Sponsorship System (TASS) to apply for a Common Access Card (CAC) for their employees that require access to a USCG or other federally controlled computer information system.

The Contractor shall submit a list of employees to the Contracting Officer's Representative (COR) for the TASS within 3 days after contract award.

Issuance of a CAC is contingent upon having a favorable NACI or equivalent investigation.

Contractor and subcontractor employees requiring access to a USCG, DOD, or other federally controlled computer information system and/or facility, or need Public Key Infrastructure authentication to perform their contractual duties shall use TASS to obtain a CAC.

The Contractor shall provide such forms to or request such information from Contractor employees that may be necessary for obtaining a CAC via the TASS. Completed forms and information shall be submitted as directed by the COR. Contractors are responsible for the accuracy and completeness of the information submitted and for any liability resulting from the Government's reliance on inaccurate or incomplete information.

Contractor or subcontractor employees who are declined a CAC via the TASS are ineligible to perform work that requires a CAC under this contract. When an employee with a CAC is no longer performing work under this contract, the Contractor shall notify the COR on the same day the employee stops working and shall deliver the CAC to the COR within seven (7) calendar days after such notification.

**1.7 PERIOD OF PERFORMANCE.** This contract consists of a base period of one year plus four one-year option periods for managing the service, for a total potential period of five years (60 months), if all options are exercised.

| | |
|---|---|
| Base Period: | 16 May 2019 – 15 May 2020 (12 Months) |
| Option Period 1: | 16 May 2020 – 15 May 2021 (12 Months) |
| Option Period 2: | 16 May 2021 – 15 May 2022 (12 Months) |
| Option Period 3: | 16 May 2022 – 15 May 2023 (12 Months) |
| Option Period 4: | 16 May 2023 – 15 May 2024 (12 Months) |

**1.8 PLACE OF PERFORMANCE.** This work will be performed at the following locations:
Primary work location:

- Contractor Facility as needed.

Alternate work locations where in-person meetings, demonstrations, and/or briefs may occur:

- U.S. Coast Guard C4ITSC at 7323 Telegraph Road, Alexandria, VA 22315
- U.S. Coast Guard C4ITSC at 408 Coast Guard Drive, Kearneysville, WV 25430
- U.S. Coast Guard C4ITSC at USCG Headquarters, 2703 Martin Luther King Jr. Ave SE, Washington, DC 20593.
- Additional locations may be added during the performance of this order.

**1.9 HOURS OF OPERATION.** Normal duty hours for the Government are Monday through Friday, 8:00AM to 5:00PM Eastern Standard Time (EST), excluding Federal Government holidays. The contractor shall be available during this time period, but also available to support any outages to the systems on a 24x7 basis. It is the expectation of the government that the systems are built in such a way that they do not go down and therefore this support should be minimal.

**1.10 CONTRACT TYPE:** BPA Call CLINs for implementation and support service will be Firm-Fixed Price (FFP). CLINs for travel will be Time & Materials without G&A.

**1.11 DELIVERABLES AND REPORTING REQUIREMENTS:** See Section 5.0 below.

**1.12 PROTECTION OF INFORMATION.**

**1.12.1 PRIVACY ACT INFORMATION.** Contractor access to information protected under the Privacy Act may be required under this contract. Contractor employees shall safeguard this information against unauthorized disclosure or dissemination in accordance with the law and Government policy and regulation.

**1.12.2 Personally Identifiable Information.**

- The contractors will cooperate with and exchange information with USCG officials, as determined necessary in order to effectively report and manage a suspected or confirmed breach.
- The contractors and subcontractors (at any tier) will properly encrypt PII in accordance with OMB Circular A-130 and other applicable policies and comply with any USCG-specific policies for protecting PII;
- Regular training for contractors and subcontractors will be conducted (at any tier) on how to identify and report a breach;
- Contractors and subcontractors (at any tier) will report a suspected or confirmed breach in any medium or form, including paper, oral, and electronic, as soon as possible and without unreasonable delay, consistent with the USCG's incident management policy and US-CERT notification guidelines;

- Contractors and subcontractors (at any tier) will maintain capabilities to determine what Federal information was or could have been access and by whom, construct a timeline of user activity, determine methods and techniques used to access Federal information, and identify the initial attack vector;
- Contractors will allow for an inspection, investigation, forensic analysis, and any other action necessary to ensure compliance with this Memorandum, the agency's breach response plan, and to assist with respond to a breach;
- Identify roles and responsibilities, and the USCG's breach response plan; and
- Explain that a report of a breach shall not, by itself, be interpreted as evidence that the contractor or its subcontractor (at any tier) failed to provide adequate safeguards for PII.

**1.12.3 PROPRIETARY INFORMATION:** Contractor access to proprietary information may be required for this contract. Contractor employees shall safeguard this information against unauthorized disclosure or dissemination in accordance with DHS MD 11042.1, Safeguarding Sensitive but Unclassified (SBU) Information. SBU includes information categorized by DHS or other government agencies as: For Official Use Only (FOUO); Official Use Only (OUO); Sensitive Homeland Security Information (SHSI); Limited Official Use (LOU); Law Enforcement Sensitive (LES); Safeguarding Information (SGI); Unclassified Controlled Nuclear Information (UCNI); and any other identifier used by other government agencies to categorize information as sensitive but unclassified. The Contractor shall ensure that all Contractor personnel having access to business or procurement sensitive information sign a non-disclosure agreement (DHS Form 11000-6). The Contractor shall continue to ensure employees safeguard this information when the new Controlled Unclassified Information (CUI) framework replaces the sensitive but unclassified (SBU) categorization.

**1.13 TRAVEL**. Contractor travel may be required to support the various BPA calls. All travel required by the Government outside the local commuting area(s) will be reimbursed to the Contractor in accordance with the Federal Acquisition Regulation (FAR) 31.205-46 - Travel Costs. The Contractor shall be responsible for obtaining COR approval via electronic mail, for all reimbursable travel. The Contractor shall submit on a monthly basis, a travel request for anticipated travel for the month travel is to be conducted.

The Contractor shall include a trip report with the monthly travel invoice to the COR and KO via electronic mail no later than five (5) business days after all travel has been conducted for that month.

**2.0 Government Furnished Property/Resources and Information.** The Government will provide access to a work area at the Government's facility as needed for the duration of this contract. This includes access to unclassified USCG workstation/laptop computers with CGONENet access as needed to meet requirements of this contract.

**3.0 CONTRACTOR FURNISHED PROPERTY: N/A**

**4.0 DELIVERABLES:**

**4.1 STATUS MEETINGS:** The Contractor shall be available to meet with the Contracting Officer and COR upon request to discuss progress, exchange information and resolve emergent technical problems and issues. These meeting shall take place at USCG's facilities and/or via telephone conference call. A mutual effort will be made to resolve all problems identified during these meetings. Specific status meetings and reports will be identified in the individual calls.

**4.2 GENERAL REPORTING REQUIREMENTS:** The Contractor shall provide all written reports in electronic format with read/write capability using applications that are compatible with USCG Standard Workstation.

**4.3 BPA CALL DELIVERABLES**: Each BPA Call will identify specific deliverables.

## 5.0 REFERENCES

- Section 508 Accessibility Standards
- Federal Information Security Management Act (FISMA)
- Privacy Act of 1974
- Clinger-Cohen Act (CCA)
- Department of Defense Instruction (DODI) 8510.01 Risk Management Framework (RMF) for DoD Information Technology (IT)
- DHS 4300A – Sensitive Systems Handbook
- NIST 800-53 (series) – Security and Privacy Controls for Federal Information Systems and Organizations
- NIST 800-146 – Cloud Computing Synopsis and Recommendations

## 6.0 GOVERNMENT POINTS OF CONTACT:

Contracting Officer's Representative (COR):
The COR and their contact information will be provided upon award.

Contracting Officer:
Brenda Oberholzer; 304-433-3223 (PH), 304-264-3817 (FX); e-mail:
Brenda.E.Oberholzer@uscg.mil

## 7.0 PAYMENT INFORMATION

The Debt Collection Improvement Act of 1996 requires Federal agencies to convert from payment by check to payment by Electronic Funds Transfer (EFT) by January 1, 1999. This requirement will eventually cover all recipients of Federal payments other than payments under the Internal Revenue Code of 1986. This notice complies with the contract clauses at Federal Acquisition Regulation (FAR) 52.232-33 "Mandatory Information for Electronic Funds Transfer Payment" and 52.232-34 "Optional Information for Electronic Funds Transfer Payment."
The USCG requires the Contractor to submit certain information to the USCG Finance Center in order to facilitate Electronic Funds Transfer (EFT) payment for deliveries or performance under this Order. Accordingly, prior to submitting the first invoice for payment, the Contractor shall

complete the attached EFT/ACH Vendor Payment Enrollment Form. The form shall be provided directly to the USCG Finance Center ("payment office") at the address below:

Commanding Officer
USCG Finance Center
1430A Kristina Way
Chesapeake, VA 23326

## 8.0 CENTRALIZED INVOICE SUBMITTAL INSTRUCTIONS

a) Each invoice shall contain the following information:

1) Contract or Delivery/Task Order Number
2) Name of the Contract Specialist or Contracting Officer
3) Invoice Routing Code (IRC) assigned by the USCG
4) Annotate on the invoice indicating that the contractor represents a small business for accelerated payment purposes.

b) The USCG unique Invoice Routing Code (IRC) for this contract or delivery/task order is: "OSC"

The IRC list may be found at http://cgweb.fincen.uscg.mil/centralinv/ under "WINS Remote Site Invoice Routing Code (IRC) Lookup"

c) Each invoice and all supporting documentation must be submitted to the designated billing office via one of the following modes, listed in descending order of preference:

1) FINCEN Website invoice receipt form: http://www.fincen.uscg.mil/centralinv/central_inv_contr.cfm
2) Fax: (757-523-6900)
3) Mailed to: Commercial Invoices
U.S. Coast Guard Finance Center
1430A Kristina Way
Chesapeake, VA 23326

d) Invoices and any supporting documentation should be submitted electronically. This will utilize the FINCEN web based invoice submission capability and facilitate processing. The invoice must be submitted as a single Adobe .pdf formatted file (not to exceed 3 MB), or as otherwise specified in the contract.

e) A courtesy copy of the invoice, **along with all supporting documentation** must also be e-mailed to the Contracting Officer and/or Contract Specialist, and the OSC centralized invoice inbox at the addresses cited below:

Brenda.E.Oberholzer@uscg.mil (Contracting Officer)

OSC-DG-INV@uscg.mil (OSC invoice inbox)

f) In accordance with the Prompt Payment Act, for the purposes of determining a payment due date and the date on which interest will begin to accrue if a payment is late, a proper invoice shall be deemed to have been received:

1) On the later of:
(i) For invoices that are mailed or transmitted via facsimile, the date a proper invoice is actually received by the designated billing office and annotates the invoice with date of receipt at the time of receipt.
(ii) For invoices electronically transmitted by the contractor via web based submission, the date a transmission is received by the designated billing office, and receipt confirmation is provided to the designated recipient; or
(ii) The seventh day after the date on which the property is actually delivered or performance of the services is actually completed; unless—
    a) The agency has actually accepted the property or services before the seventh day in which case the acceptance date shall substitute for the seventh day after the delivery date; or
    b) A longer acceptance period is specified in the contract, in which case the date of actual acceptance or the date on which such longer acceptance period ends shall substitute for the seventh day after the delivery date;

2) On the date placed on the invoice by the contractor, when the agency fails to annotate the invoice with date of receipt of the invoice at the time of receipt (such invoice must be a proper invoice); or

3) On the date of delivery, when the contract specifies that the delivery ticket may serve as an invoice.

4) Web based submission by the contractor and receipt confirmation does not reflect Government review or acceptance of the invoice.

5) Payment inquiries and status may be obtained - at the following website: - https://www.fincen.uscg.mil/secure/payment.htm.

**In addition to the clauses set forth in the Contractor's Federal Supply Schedule (FSS) Contract, the following additional clauses are herein made a part of, and pertain to, any resultant contract action for this BPA.**

## FEDERAL ACQUISITION REGULATION CLAUSES INCORPORATED BY REFERENCE

| CLAUSE NO. | CLAUSE TITLE | DATE |
|---|---|---|
| 52.203-13 | Contractor Code of Business Ethics and Conduct | OCT 2015 |
| 52.204-7 | System for Award Management | OCT 2016 |
| 52.204-9 | Personal Identity Verification of Contractor Personnel | JAN 2011 |
| 52.204-16 | Commercial and Government Entity Code Reporting | JUL 2016 |
| 52.204-17 | Ownership or Control of Offeror | JUL 2016 |
| 52.204-18 | Commercial and Government Entity Code Maintenance | JUL 2016 |
| 52.204-19 | Incorporation by Reference of Representations and Certifications | DEC 2014 |
| 52.204-21 | Basic Safeguarding of Covered Contractor Information Systems | JUN 2016 |
| 52.209-11 | Representation by Corporations Regarding Delinquent Tax Liability or a Felony Conviction under any Federal Law | FEB 2016 |
| 52.212-1 | Instructions to Offerors--Commercial Items | JAN 2017 |
| 52.212-4 | Contract Terms and Conditions--Commercial Items | JAN 2017 |
| 52.217-5 | Evaluation of Options | JUL 1990 |
| 52.224-2 | Privacy Act | APR 1984 |
| 52.225-25 | Prohibition on Contracting with Entities Engaging in Certain Activities or Transactions Relating to Iran—Representation and Certifications | OCT 2015 |
| 52.227-14 | Rights in Data – General (Alternative IV) | DEC 2007 |
| 52.227-16 | Additional Data Requirements | JUN 1987 |
| 52.227-19 | Commercial Computer Software—Restricted Rights | DEC 2007 |
| 52.232-18 | Availability of Funds | APR 1984 |
| 52.232-39 | Unenforceability of Unauthorized Obligations | JUN 2013 |
| 52.237-3 | Continuity of Services | JAN 1991 |
| 52.245-1 | Government Property | JAN 2017 |
| 52.245-9 | Use and Charges | APR 2012 |

## FEDERAL ACQUISITION REGULATION CLAUSES INCORPORATED BY FULL TEXT

### 52.203-17 – Contractor Employee Whistleblower Rights and Requirement To Inform Employees of Whistleblower Rights (APR 2014)

(a) This contract and employees working on this contract will be subject to the whistleblower rights and remedies in the pilot program on Contractor employee whistleblower protections established at 41 U.S.C. 4712 by section 828 of the National Defense Authorization Act for Fiscal Year 2013 (Pub. L. 112-239) and FAR 3.908.

(b) The Contractor shall inform its employees in writing, in the predominant language of the workforce, of employee whistleblower rights and protections under 41 U.S.C. 4712, as described in section 3.908 of the Federal Acquisition Regulation.

(c) The Contractor shall insert the substance of this clause, including this paragraph (c), in all subcontracts over the simplified acquisition threshold.

**(End of clause)**

**52.204-2 SECURITY REQUIREMENTS (AUG 1996)**

(a) This clause applies to the extent that this contract involves access to information classified "Confidential," "Secret," or "Top Secret."

(b) The Contractor shall comply with—

(1) The Security Agreement (**DD Form 441**), including the National Industrial Security Program Operating Manual (DoD 5220.22-M); and

(2) Any revisions to that manual, notice of which has been furnished to the Contractor.

(c) If, subsequent to the date of this contract, the security classification or security requirements under this contract are changed by the Government and if the changes cause an increase or decrease in security costs or otherwise affect any other term or condition of this contract, the contract shall be subject to an equitable adjustment as if the changes were directed under the Changes clause of this contract.

(d) The Contractor agrees to insert terms that conform substantially to the language of this clause, including this paragraph (d) but excluding any reference to the Changes clause of this contract, in all subcontracts under this contract that involve access to classified information.

**(End of clause)**

**52.204-15 Service Contract Reporting Requirements for Indefinite-Delivery Contracts (OCT 2016)**

(a) *Definition.*

"First-tier subcontract" means a subcontract awarded directly by the Contractor for the purpose of acquiring supplies or services (including construction) for performance of a prime contract. It does not include the Contractor's supplier agreements with vendors, such as long-term arrangements for materials or supplies that benefit multiple contracts and/or the costs of which are normally applied to a Contractor's general and administrative expenses or indirect costs.

(b) The Contractor shall report, in accordance with paragraphs (c) and(d) of this clause, annually by October 31, for services performed during the preceding Government fiscal year (October1-September 30) under this contract for orders that exceed the thresholds established in 4.1703(a)(2).

(c) The Contractor shall report the following information:

(1) Contract number and order number.

(2) The total dollar amount invoiced for services performed during the previous Government fiscal year under the order.

(3) The number of Contractor direct labor hours expended on the services performed during the previous Government fiscal year.

(4) Data reported by subcontractors under paragraph (f) of this clause.

(d) The information required in paragraph (c) of this clause shall be submitted via the internet at www.sam.gov. (See SAM User Guide). If the Contractor fails to submit the report in a timely manner, the contracting officer will exercise appropriate contractual remedies. In addition, the Contracting Officer will make the Contractor's failure to comply with the reporting requirements a part of the Contractor's performance information under FAR subpart 42.15.

(e) Agencies will review Contractor reported information for reasonableness and consistency with available contract information. In the event the agency believes that revisions to the Contractor reported information are warranted, the agency will notify the Contractor no later than November 15. By November 30, the Contractor shall revise the report or document its rationale for the agency.

(f)

(1) The Contractor shall require each first-tier subcontractor providing services under this contract, with subcontract(s) each valued at or above the thresholds set forth in 4.1703(a)(2), to provide the following detailed information to the Contractor in sufficient time to submit the report:

(i) Subcontract number (including subcontractor name and unique entity identifier), and

(ii) The number of first-tier subcontractor direct-labor hours expended on the services performed during the previous Government fiscal year.

(2) The Contractor shall advise the subcontractor that the information will be made available to the public as required by section 743 of Division C of the Consolidated Appropriations Act, 2010.

**(End of clause)**

**52.209-7 Information Regarding Responsibility Matters (JUL 2013)**

(a) *Definitions*. As used in this provision—

"Administrative proceeding" means a non-judicial process that is adjudicatory in nature in order to make a determination of fault or liability (*e.g.*, Securities and Exchange Commission Administrative Proceedings, Civilian Board of Contract Appeals Proceedings, and Armed Services Board of Contract Appeals Proceedings). This includes administrative proceedings at the Federal and State level but only in connection with performance of a Federal contract or grant. It does not include agency actions such as contract audits, site visits, corrective plans, or inspection of deliverables.

"Federal contracts and grants with total value greater than $10,000,000" means—

(1) The total value of all current, active contracts and grants, including all priced options; and

(2) The total value of all current, active orders including all priced options under indefinite-delivery, indefinite-quantity, 8(a), or requirements contracts (including task and delivery and multiple-award Schedules).

"Principal" means an officer, director, owner, partner, or a person having primary management or supervisory responsibilities within a business entity (*e.g.*, general manager; plant manager; head of a division or business segment; and similar positions).

(b) The offeror [ ] has [ ] does not have current active Federal contracts and grants with total value greater than $10,000,000.

(c) If the offeror checked "has" in paragraph (b) of this pro- vision, the offeror represents, by submission of this offer, that the information it has entered in the Federal Awardee Performance and Integrity Information System (FAPIIS) is current, accurate, and complete as of the date of submission of this offer with regard to the following information:

(1) Whether the offeror, and/or any of its principals, has or has not, within the last five years, in connection with the award to or performance by the offeror of a Federal contract

or grant, been the subject of a proceeding, at the Federal or State level that resulted in any of the following dispositions:

(i) In a criminal proceeding, a conviction.

(ii) In a civil proceeding, a finding of fault and liability that results in the payment of a monetary fine, penalty, reimbursement, restitution, or damages of $5,000 or more.

(iii) In an administrative proceeding, a finding of fault and liability that results in—

(A) The payment of a monetary fine or penalty of $5,000 or more; or

(B) The payment of a reimbursement, restitution, or damages in excess of $100,000.

(iv) In a criminal, civil, or administrative proceeding, a disposition of the matter by consent or compromise with an acknowledgment of fault by the Contractor if the proceeding could have led to any of the outcomes specified in paragraphs (c)(1)(i), (c)(1)(ii), or (c)(1)(iii) of this provision.

(2) If the offeror has been involved in the last five years in any of the occurrences listed in (c)(1) of this provision, whether the offeror has provided the requested information with regard to each occurrence.

(d) The offeror shall post the information in paragraphs (c)(1)(i) through (c)(1)(iv) of this provision in FAPIIS as required through maintaining an active registration in the System for Award Management database via https:// www.acquisition.gov (see 52.204-7).

**(End of provision)**

**52.209-9 Updates of Publicly Available Information Regarding Responsibility**

**Matters (JUL 2013)**

(a) The Contractor shall update the information in the Federal Awardee Performance and Integrity Information System (FAPIIS) on a semi-annual basis, throughout the life of the contract, by posting the required information in the System for Award Management database via https://www.acquisition.gov.

(b) As required by section 3010 of the Supplemental Appropriations Act, 2010 (Pub. L. 111-212), all information posted in FAPIIS on or after April 15, 2011, except past performance

reviews, will be publicly available. FAPIIS consists of two segments—

(1) The non-public segment, into which Government officials and the Contractor post information, which can only be viewed by—

(i) Government personnel and authorized users performing business on behalf of the Government; or

(ii) The Contractor, when viewing data on itself; and

(2) The publicly-available segment, to which all data in the non-public segment of FAPIIS is automatically transferred after a waiting period of 14 calendar days, except for—

(i) Past performance reviews required by subpart 42.15;

(ii) Information that was entered prior to April 15, 2011; or

(iii) Information that is withdrawn during the 14-calendar-day waiting period by the Government official who posted it in accordance with paragraph (c)(1) of this clause.

(c) The Contractor will receive notification when the Government posts new information to the Contractor's record.

(1) If the Contractor asserts in writing within 7 calendar days, to the Government official who posted the information, that some of the information posted to the non-public segment of FAPIIS is covered by a disclosure exemption under the Freedom of Information Act, the Government official who posted the information must within 7 calendar days remove the posting from FAPIIS and resolve the issue in accordance with agency Freedom of Information procedures, prior to reposting the releasable information. The contractor must cite 52.209-9 and request removal within 7 calendar days of the posting to FAPIIS.

(2) The Contractor will also have an opportunity to post comments regarding information that has been posted by the Government. The comments will be retained as long as the associated information is retained, i.e., for a total period of 6 years. Contractor comments will remain a part of the record unless the Contractor revises them.

(3) As required by section 3010 of Pub. L. 111-212, all information posted in FAPIIS on or after April 15, 2011, except past performance reviews, will be publicly available.

(d) Public requests for system information posted prior to April 15, 2011, will be handled under Freedom of Information Act procedures, including, where appropriate, procedures promulgated under E.O. 12600.

**(End of clause)**

**52.212-3 Offeror Representations and Certifications--Commercial Items, Alternate I (NOV 2017)**

The offeror shall complete only paragraphs (b) of this provision if the Offeror has completed the annual representations and certification electronically via the System for Award Management (SAM) Web site located at https://www.sam.gov/portal. If the Offeror has not

completed the annual representations and certifications electronically, the Offeror shall complete only paragraphs (c) through (t) of this provision.

(a) *Definitions.* As used in this provision—

*"Economically disadvantage women-owned small business (EDWOSB) concern"* means a small business concern that is at least 51 percent directly and unconditionally owned by, and the management and daily business operations of which are controlled by, one or more women who are citizens of the United States and who are economically disadvantaged in accordance with 13 CFR part 127. It automatically qualifies as a women-owned small business eligible under the WOSB Program.

*"Highest-level owner"* means the entity that owns or controls an immediate owner of the offeror, or that owns or controls one or more entities that control an immediate owner of the offeror. No entity owns or exercises control of the highest level owner.

*"Immediate owner"* means an entity, other than the offeror, that has direct control of the offeror. Indicators of control include, but are not limited to, one or more of the following: Ownership or interlocking management, identity of interests among family members, shared facilities and equipment, and the common use of employees.

*"Inverted domestic corporation"* means a foreign incorporated entity that meets the definition of an inverted domestic corporation under 6 U.S.C. 395(b), applied in accordance with the rules and definitions of 6 U.S.C. 395(c).

*"Manufactured end product"* means any end product and service codes (PSCs) 1000-9999, except—

(1) PSC 5510, Lumber and Related Basic Wood Materials;

(2) Product or Service Group (PSG) 87, Agricultural Supplies;

(3) PSG 88, Live Animals;

(4) PSG 89, Subsistence;

(5) PSC 9410, Crude Grades of Plant Materials;

(6) PSC 9430, Miscellaneous Crude Animal Products, Inedible;

(7) PSC 9440, Miscellaneous Crude Agricultural and Forestry Products;

(8) PSC 9610, Ores;

(9) PSC 9620, Minerals, Natural and Synthetic; and

(10) PSC 9630, Additive Metal Materials.

*"Place of manufacture"* means the place where an end product is assembled out of components, or otherwise made or processed from raw materials into the finished product that is to be provided to the Government. If a product is disassembled and reassembled, the place of reassembly is not the place of manufacture.

*"Predecessor"* means an entity that is replaced by a successor and includes any predecessors of the predecessor.

*"Restricted business operations"* means business operations in Sudan that include power production activities, mineral extraction activities, oil-related activities, or the production of military equipment, as those terms are defined in the Sudan Accountability and Divestment Act of 2007 (Pub. L. 110-174). Restricted business operations do not include business operations that the person (as that term is defined in Section 2 of the Sudan Accountability and Divestment Act of 2007) conducting the business can demonstrate—

(1) Are conducted under contract directly and exclusively with the regional government of southern Sudan;

(2) Are conducted pursuant to specific authorization from the Office of Foreign Assets Control in the Department of the Treasury, or are expressly exempted under Federal law from the requirement to be conducted under such authorization;

(3) Consist of providing goods or services to marginalized populations of Sudan;

(4) Consist of providing goods or services to an internationally recognized peacekeeping force or humanitarian organization;

(5) Consist of providing goods or services that are used only to promote health or education; or

(6) Have been voluntarily suspended.

"*Sensitive technology"*—

(1) Means hardware, software, telecommunications equipment, or any other technology that is to be used specifically--

(i) To restrict the free flow of unbiased information in Iran; or

(ii) To disrupt, monitor, or otherwise restrict speech of the people of Iran; and

(2) Does not include information or informational materials the export of which the President does not have the authority to regulate or prohibit pursuant to section

203(b)(3) of the International Emergency Economic Powers Act (50 U.S.C. 1702(b)(3)).

*"Service-disabled veteran-owned small business concern"*--

(1) Means a small business concern--

(i) Not less than 51 percent of which is owned by one or more service--disabled veterans or, in the case of any publicly owned business, not less than 51 percent of the stock of which is owned by one or more service-disabled veterans; and

(ii) The management and daily business operations of which are controlled by one or more service-disabled veterans or, in the case of a service-disabled veteran with permanent and severe disability, the spouse or permanent caregiver of such veteran.

(2) "Service-disabled veteran" means a veteran, as defined in 38 U.S.C. 101(2), with a disability that is service-connected, as defined in 38 U.S.C. 101(16).

*"Small business concern"* 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 criteria in 13 CFR Part 121 and size standards in this solicitation.

"*Small disadvantaged business concern, consistent with 13 CFR 124.1002,"* means a small business concern under the size standard applicable to the acquisition, that--

(1) Is at least 51 percent unconditionally and directly owned (as defined at 13 CFR 124.105) by--

(i) One or more socially disadvantaged (as defined at 13 CFR 124.103) and economically disadvantaged (as defined at 13 CFR 124.104) individuals who are citizens of the United States; and

(ii) Each individual claiming economic disadvantage has a net worth not exceeding $750,000 after taking into account the applicable exclusions set forth at 13 CFR 124.104(c)(2); and

(2) The management and daily business operations of which are controlled (as defined at 13.CFR 124.106) by individuals, who meet the criteria in paragraphs (1)(i) and (ii) of this definition.

*"Subsidiary"* means an entity in which more than 50 percent of the entity is owned—

(1) Directly by a parent corporation; or

(2) Through another subsidiary of a parent corporation.

"*Successor*" means an entity that has replaced a predecessor by acquiring the assets and carrying out the affairs of the predecessor under a new name (often through acquisition or merger). The term "successor" does not include new offices/divisions of the same company or a company that only changes its name. The extent of the responsibility of the successor for the liabilities of the predecessor may vary, depending on State law and specific circumstances.

*"Veteran-owned small business concern"* means a small business concern--

(1) Not less than 51 percent of which is owned by one or more veterans (as defined at 38 U.S.C. 101(2)) or, in the case of any publicly owned business, not less than 51 percent of the stock of which is owned by one or more veterans; and

(2) The management and daily business operations of which are controlled by one or more veterans.

*"Women-owned business concern"* means a concern which is at least 51 percent owned by one or more women; or in the case of any publicly owned business, at least 51 percent of its stock is owned by one or more women; and whose management and daily business operations are controlled by one or more women.

*"Women-owned small business concern"* means a small business concern--

(1) That is at least 51 percent owned by one or more women; or in the case of any publicly owned business, at least 51 percent of the stock of which is owned by one or more women; and

(2) Whose management and daily business operations are controlled by one or more women.

*"Women-owned small business (WOSB) concern eligible under the WOSB Program (in accordance with 13 CFR part 127),"* means a small business concern that is at least 51 percent directly and unconditionally owned by, and the management and daily business operations of which are controlled by, one or more women who are citizens of the United States.

(b)(1) *Annual Representations and Certifications*. Any changes provided by the offeror in paragraph (b)(2) of this provision do not automatically change the representations and certifications posted on the SAM website.

(2) The offeror has completed the annual representations and certification electronically via the SAM website accessed through http://www.acquisition.gov . After reviewing the SAM database information, the offeror verifies by submission of this offer that the representation and certifications currently posted electronically at FAR 52.212-3, Offeror Representations and Certifications—Commercial Items, have been entered or updated in the last 12 months, are current, accurate, complete, and applicable to this solicitation (including the business size standard applicable to the NAICS code referenced for this solicitation), as of the date of this offer and are incorporated in this offer by reference (see FAR 4.1201), except for paragraphs _____. *[Offeror to identify the applicable paragraphs at (c) through (s) of this provision that the offeror has completed for the purposes of this solicitation only, if any. These amended representation(s) and/or certification(s) are also incorporated in this offer and are current, accurate, and complete as of the date of this offer. Any changes provided by the offeror are applicable to this solicitation only, and do not result in an update to the representations and certifications posted electronically on SAM.]*

(c) Offerors must complete the following representations when the resulting contract will be performed in the United States or its outlying areas. Check all that apply.

(1) *Small business concern*. The offeror represents as part of its offer that it **[ ] is, [ ] is not** a small business concern.

(2) *Veteran-owned small business concern. [Complete only if the offeror represented itself as a small business concern in paragraph (c)(1) of this provision.]* The offeror represents as part of its offer that it **[ ] is, [ ] is not** a veteran-owned small business concern.

(3) *Service-disabled veteran-owned small business concern. [Complete only if the offeror represented itself as a veteran-owned small business concern in paragraph (c)(2) of this provision.]* The offeror represents as part of its offer that it **[ ] is, [ ] is not** a service-disabled veteran-owned small business concern.

(4) *Small disadvantaged business concern. [Complete only if the offeror represented itself as a small business concern in paragraph (c)(1) of this provision.]* The offeror represents that it **[ ] is, [ ] is not** a small disadvantaged business concern as defined in 13 CFR 124.1002.

(5) *Women-owned small business concern. [Complete only if the offeror represented itself as a small business concern in paragraph (c)(1) of this provision.]*

The offeror represents that it **[ ] is, [ ] is not** a women-owned small business

concern.

**Note:** Complete paragraphs (c)(8) and (c)(9) only if this solicitation is expected to exceed the simplified acquisition threshold.

(6) *WOSB concern eligible under the WOSB Program. [Complete only if the offeror represented itself as a women-owned small business concern in paragraph (c)(5) of this provision.]* The offeror represents that—

(i) It **[ ] is, [ ] is not** a WOSB concern eligible under the WOSB Program, has provided all the required documents to the WOSB Repository, and no change in circumstances or adverse decisions have been issued that affects its eligibility; and

(ii) It **[ ] is, [ ] is not** a joint venture that complies with the requirements of 13 CFR part 127, and the representation in paragraph (c)(6)(i) of this provision is accurate for each WOSB concern eligible under the WOSB Program participating in the joint venture. *[The offeror shall enter the name or names of the WOSB concern eligible under the WOSB Program and other small businesses that are participating in the joint venture: _____.]* Each WOSB concern eligible under the WOSB Program participating in the joint venture shall submit a separate signed copy of the WOSB representation.

(7) *Economically disadvantaged women-owned small business (EDWOSB) concern. [Complete only if the offeror represented itself as a WOSB concern eligible under the WOSB Program in (c)(6) of this provision.]* The offeror represents that—

(i) It **[ ] is, [ ] is not** an EDWOSB concern, has provided all the required documents to the WOSB Repository, and no change in circumstances or adverse decisions have been issued that affects its eligibility; and

(ii) It **[ ] is, [ ] is not** a joint venture that complies with the requirements of 13 CFR part 127, and the representation in paragraph (c)(7)(i) of this provision is accurate for each EDWOSB concern participating in the joint venture. *[The offeror shall enter the name or names of the EDWOSB concern and other small businesses that are participating in the joint venture: _____.]* Each EDWOSB concern participating in the joint venture shall submit a separate signed copy of the EDWOSB representation.

(8) *Women-owned business concern (other than small business concern). [Complete only if the offeror is a women-owned business concern and did not represent itself as a small business concern in paragraph (c)(1) of this provision.]* The offeror

represents that it **[ ] is** a women-owned business concern.

(9) *Tie bid priority for labor surplus area concerns***.** If this is an invitation for bid, small business offerors may identify the labor surplus areas in which costs to be incurred on account of manufacturing or production (by offeror or first-tier subcontractors) amount to more than 50 percent of the contract price:

_____

(10) *HUBZone small business concern. [Complete only if the offeror represented itself as a small business concern in paragraph (c)(1) of this provision.]* The offeror represents, as part of its offer, that—

(i) It **[ ] is, [ ] is not** a HUBZone small business concern listed, on the date of this representation, on the List of Qualified HUBZone Small Business Concerns maintained by the Small Business Administration, and no material changes in ownership and control, principal office, or HUBZone employee percentage have occurred since it was certified in accordance with 13 CFR part 126; and

(ii) It **[ ] is, [ ] is not** a HUBZone joint venture that complies with the requirements of 13 CFR part 126, and the representation in paragraph (c)(10)(i) of this provision is accurate for each HUBZone small business concern participating in the HUBZone joint venture. *[The offeror shall enter the names of each of the HUBZone small business concerns participating in the HUBZone joint venture: _____.]* Each HUBZone small business concern participating in the HUBZone joint venture shall submit a separate signed copy of the HUBZone representation.

(c)(11) (Complete if the offeror has represented itself as disadvantaged in paragraph (c)(4) or (c)(8) of this provision.)

*[The offeror shall check the category in which its ownership falls]:*

____ Black American.

____ Hispanic American.

____ Native American (American Indians, Eskimos, Aleuts, or Native Hawaiians).

____ Asian-Pacific American (persons with origins from Burma, Thailand, Malaysia, Indonesia, Singapore, Brunei, Japan, China, Taiwan, Laos, Cambodia (Kampuchea), Vietnam, Korea, The Philippines, Republic of Palau, Republic of the Marshall

Islands, Federated States of Micronesia, the Commonwealth of the Northern Mariana Islands, Guam, Samoa, Macao, Hong Kong, Fiji, Tonga, Kiribati, Tuvalu, or Nauru).

____ Subcontinent Asian (Asian-Indian) American (persons with origins form India, Pakistan, Bangladesh, Sri Lanka, Bhutan, the Maldives Islands, or Nepal).

____ Individual/concern, other than one of the preceding.

(d) *Representations required to implement provisions of Executive Order 11246--*

(1) Previous Contracts and Compliance. The offeror represents that--

(i) It **[ ] has, [ ] has not** participated in a previous contract or subcontract subject either to the Equal Opportunity clause of this solicitation; and

(ii) It **[ ] has, [ ] has not** filed all required compliance reports.

(2) *Affirmative Action Compliance.* The offeror represents that--

(i) It **[ ] has** developed and has on file, **[ ] has not** developed and does not have on file, at each establishment, affirmative action programs required by rules and regulations of the Secretary of Labor (41 CFR parts 60-1 and 60-2), or

(ii) It **[ ] has not** previously had contracts subject to the written affirmative action programs requirement of the rules and regulations of the Secretary of Labor.

(e) *Certification Regarding Payments to Influence Federal Transactions (31 U.S.C. 1352).* (Applies only if the contract is expected to exceed $150,000.) By submission of its offer, the offeror certifies to the best of its knowledge and belief that no Federal appropriated funds have been paid or will be paid to any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress or an employee of a Member of Congress on his or her behalf in connection with the award of any resultant contract. If any registrants under the Lobbying Disclosure Act of 1995 have made a lobbying contact on behalf of the offeror with respect to this contract, the offeror shall complete and submit, with its offer, OMB Standard Form LLL Disclosure of Lobbying Activities, to provide the name of the registrants. The offeror need not report regularly employed officers or employees of the offeror to whom payment of reasonable compensation were made.

(f) *Buy American Certificate*. **(Applies only if the clause at Federal Acquisition Regulation (FAR) 52.225-1, Buy American--Supplies, is included in this solicitation.)**

(1) The offeror certifies that each end product, except those listed in paragraph (f)(2) of this provision, is a domestic end product and that for other than COTS items, the offeror has considered components of unknown origin to have been mined, produced, or manufactured outside the United States. The offeror shall list as foreign end products those end products manufactured in the United States that do not qualify as domestic end products, *i.e.*, an end product that is not a COTS item and does not meet the component test in paragraph (2) of the definition of "domestic end product," The terms "commercially available off-the-shelf (COTS) item," "component," "domestic end product," "end product," "foreign end product," and "United States" are defined in the clause of this solicitation entitled "Buy American—Supplies."

(2) **Foreign End Products:**

| Line Item No. | Country Of Origin |
|---|---|
| _____ | _____ |
| _____ | _____ |

[List as necessary]

(3) The Government will evaluate offers in accordance with the policies and procedures of FAR Part 25.

(g) (1) *Buy American--Free Trade Agreements—Israeli Trade Act Certificate.* **(Applies only if the clause at FAR 52.225-3, Buy American--Free Trade Agreements--Israeli Trade Act, is included in this solicitation.)**

(i) The offeror certifies that each end product, except those listed in paragraph (g)(1)(ii) or (g)(1)(iii) of this provision, is a domestic end product and that for other than COTS items, the offeror has considered components of unknown origin to have been mined, produced, or manufactured outside the United States. The terms "Bahrainian, Moroccan, Omani, Panamanian, or Peruvian end product," "commercially available off-the-shelf (COTS) item," "component," "domestic end product," "end product," "foreign end product," "Free Trade Agreement country," "Free Trade Agreement country end product," "Israeli end product," and "United States" are defined in the clause of this solicitation entitled "Buy American—Free Trade Agreements—Israeli Trade Act."

(ii) The offeror certifies that the following supplies are Free Trade Agreement country end products (other than Bahrainian, Moroccan, Omani, Panamanian, or Peruvian end products) or Israeli end products as defined in the clause of

this solicitation entitled “Buy American--Free Trade Agreements--Israeli Trade Act”:

**Free Trade Agreement Country End Products (Other than Bahrainian, Moroccan, Omani, Panamanian, or Peruvian End Products) or Israeli End Products:**

| Line Item No. | Country Of Origin |
|---|---|
| _____ | _____ |
| _____ | _____ |

[List as necessary]

(iii) The offeror shall list those supplies that are foreign end products (other than those listed in paragraph (g)(1)(ii) of this provision) as defined in the clause of this solicitation entitled "Buy American--Free Trade Agreements--Israeli Trade Act.” The offeror shall list as other foreign end products those end products manufactured in the United States that do not qualify as domestic end products, *i.e.*, an end product that is not a COTS item and does not meet the component test in paragraph (2) of the definition of “domestic end product.”

**Other Foreign End Products:**

| Line Item No. | Country Of Origin |
|---|---|
| _____ | _____ |
| _____ | _____ |

[List as necessary]

(iv) The Government will evaluate offers in accordance with the policies and procedures of FAR Part 25.

(2) *Buy American--Free Trade Agreements--Israeli Trade Act Certificate, Alternate I.* If Alternate I to the clause at FAR 52.225-3 is included in this solicitation, substitute the following paragraph (g)(1)(ii) for paragraph (g)(1)(ii) of the basic provision:

(g) (1) (ii) The offeror certifies that the following supplies are Canadian end products as defined in the clause of this solicitation entitled “Buy American--Free Trade Agreements--Israeli Trade Act":

(ii) **Canadian End Products:**

Line Item No.

_____

_____

[List as necessary]

(3) *Buy American--Free Trade Agreements--Israeli Trade Act Certificate, Alternate II.* If Alternate II to the clause at FAR 52.225-3 is included in this solicitation, substitute the following paragraph (g)(1)(ii) for paragraph (g)(1)(ii) of the basic provision:

(g) (1) (ii) The offeror certifies that the following supplies are Canadian end products or Israeli end products as defined in the clause of this solicitation entitled "Buy American--Free Trade Agreements--Israeli Trade Act":

**Canadian or Israeli End Products:**

| Line Item No. | Country Of Origin |
|---|---|
| _____ | _____ |
| _____ | _____ |

[List as necessary]

(4) *Buy American—Free Trade Agreements—Israeli Trade Act Certificate, Alternate III.* If Alternate III to the clause at 52.225-3 is included in this solicitation, substitute the following paragraph (g)(1)(ii) for paragraph (g)(1)(ii) of the basic provision:

(g) (1) (ii) The offeror certifies that the following supplies are Free Trade Agreement country end products (other than Bahrainian, Korean, Moroccan, Omani, Panamanian, or Peruvian end products) or Israeli end products as defined in the clause of this solicitation entitled "Buy American--Free Trade Agreements--Israeli Trade Act":

**Free Trade Agreement Country End Products (Other than Bahrainian, Korean, Moroccan, Omani, Panamanian, or Peruvian End Products) or Israeli End Products:**

| Line Item No. | Country Of Origin |
|---|---|

| | |
|---|---|
| _____ | _____ |
| _____ | _____ |

[List as necessary]

(5) *Trade Agreements Certificate.* **(Applies only if the clause at FAR 52.225-5, Trade Agreements, is included in this solicitation.)**

(i) The offeror certifies that each end product, except those listed in paragraph (g)(5)(ii) of this provision, is a U.S.-made or designated country end product, as defined in the clause of this solicitation entitled "Trade Agreements."

(ii) The offeror shall list as other end products those end products that are not U.S.-made or designated country end products.

**Other End Products:**

| Line Item No. | Country Of Origin |
|---|---|
| _____ | _____ |
| _____ | _____ |

[List as necessary]

(iii) The Government will evaluate offers in accordance with the policies and procedures of FAR Part 25. For line items covered by the WTO GPA, the Government will evaluate offers of U.S.-made or designated country end products without regard to the restrictions of the Buy American statute. The Government will consider for award only offers of U.S.-made or designated country end products unless the Contracting Officer determines that there are no offers for such products or that the offers for such products are insufficient to fulfill the requirements of the solicitation.

(h) *Certification Regarding Responsibility Matters (Executive Order 12689).* (Applies only if the contract value is expected to exceed the simplified acquisition threshold.) The offeror certifies, to the best of its knowledge and belief, that the offeror and/or any of its principals—

(1) **[ ] Are, [ ] are not** presently debarred, suspended, proposed for debarment, or declared ineligible for the award of contracts by any Federal agency;

(2) **[ ] Have, [ ] have not**, within a three-year period preceding this offer, been convicted of or had a civil judgment rendered against them for: Commission of fraud or a criminal offense in connection with obtaining, attempting to obtain, or

performing a Federal, state or local government contract or subcontract; violation of Federal or state antitrust statutes relating to the submission of offers; or Commission of embezzlement, theft, forgery, bribery, falsification or destruction of records, making false statements, tax evasion, violating criminal tax laws, or receiving stolen property;

(3) **[ ] Are, [ ] are not** presently indicted for, or otherwise criminally or civilly charged by a Government entity with, commission of any of these offenses enumerated in paragraph (h)(2) of this clause; and

(4) **[ ] Have, [ ] have not**, within a three-year period preceding this offer, been notified of any delinquent Federal taxes in an amount that exceeds $3,500 for which the liability remains unsatisfied.

(i) Taxes are considered delinquent if both of the following criteria apply:

(A) *The tax liability is finally determined*. The liability is finally determined if it has been assessed. A liability is not finally determined if there is a pending administrative or judicial challenge. In the case of a judicial challenge to the liability, the liability is not finally determined until all judicial appeal rights have been exhausted.

(B) *The taxpayer is delinquent in making payment*. A taxpayer is delinquent if the taxpayer has failed to pay the tax liability when full payment was due and required. A taxpayer is not delinquent in cases where enforced collection action is precluded.

(ii) *Examples*.

(A) The taxpayer has received a statutory notice of deficiency, under I.R.C. section 6212, which entitles the taxpayer to seek Tax Court review of a proposed tax deficiency. This is not a delinquent tax because it is not a final tax liability. Should the taxpayer seek Tax Court review, this will not be a final tax liability until the taxpayer has exercised all judicial appear rights.

(B) The IRS has filed a notice of Federal tax lien with respect to an assessed tax liability, and the taxpayer has been issued a notice under I.R.C. section 6320 entitling the taxpayer to request a hearing with the IRS Office of Appeals Contesting the lien filing, and to further appeal to the Tax Court if the IRS determines to sustain the lien filing. In the course of the hearing, the taxpayer is entitled to contest the underlying tax liability because the taxpayer has had no prior opportunity to

contest the liability. This is not a delinquent tax because it is not a final tax liability. Should the taxpayer seek tax court review, this will not be a final tax liability until the taxpayer has exercised all judicial appeal rights.

(C) The taxpayer has entered into an installment agreement pursuant to I.R.C. section 6159. The taxpayer is making timely payments and is in full compliance with the agreement terms. The taxpayer is not delinquent because the taxpayer is not currently required to make full payment.

(D) The taxpayer has filed for bankruptcy protection. The taxpayer is not delinquent because enforced collection action is stayed under 11 U.S.C. section 362 (the Bankruptcy Code).

(i) *Certification Regarding Knowledge of Child Labor for Listed End Products (Executive Order 13126). [The Contracting Officer must list in paragraph (j)(1) any end products being acquired under this solicitation that are included in the List of Products Requiring Contractor Certification as to Forced or Indentured Child Labor; unless excluded at 22.1503(b).]*

(1) **Listed End Products**.

| Listed End Product | Listed Countries of Origin |
|---|---|
| _____ | _____ |
| _____ | _____ |

*(2) Certification. [If the Contracting Officer has identified end products and countries of origin in paragraph (j)(1) of this provision, then the offeror must certify to either (j)(2)(i) or (j)(2)(ii) by checking the appropriate block.]*

**[ ]** (i) The offeror will not supply any end product listed in paragraph (j)(1) of this provision that was mined, produced, or manufactured in the corresponding country as listed for that product.

**[ ]** (ii) The offeror may supply an end product listed in paragraph (j)(1) of this provision that was mined, produced, or manufactured in the corresponding country as listed for that product. The offeror certifies that is has made a good faith effort to determine whether forced or indentured child labor was used to mine, produce, or manufacture any such end product furnished under this contract. On the basis of those efforts, the offeror certifies that it is not aware

of any such use of child labor.

(j) *Place of Manufacture.* (Does not apply unless the solicitation is predominantly for the acquisition of manufactured end products.) For statistical purposes only, the offeror shall indicate whether the place of manufacture of the end products it expects to provide in response to this solicitation is predominantly—

(1) **[ ]** In the United States (Check this box if the total anticipated price of offered end products manufactured in the United States exceeds the total anticipated price of offered end products manufactured outside the United States); or

(2) **[ ]** Outside the United States.

(k) *Certificates regarding exemptions from the application of the Service Contract Labor Standards*. (Certification by the offeror as to its compliance with respect to the contract also constitutes its certification as to compliance by its subcontractor if it subcontracts out the exempt services.)

(1) **[ ]** Maintenance, calibration, or repair of certain equipment as described in FAR 22.1003-4(c)(1). The offeror **[ ] does [ ] does not** certify that—

(i) The items of equipment to be serviced under this contract are used regularly for other than Governmental purposes and are sold or traded by the offeror (or subcontractor in the case of an exempt subcontract) in substantial quantities to the general public in the course of normal business operations;

(ii) The services will be furnished at prices which are, or are based on, established catalog or market prices (see FAR 22.1003-4(c)(2)(ii)) for the maintenance, calibration, or repair of such equipment; and

(iii) The compensation (wage and fringe benefits) plan for all service employees performing work under the contract will be the same as that used for these employees and equivalent employees servicing the same equipment of commercial customers.

(2) **[ ]** Certain services as described in FAR 22.1003-4(d)(1). The offeror **[ ] does [ ] does not** certify that—

(i) The services under the contract are offered and sold regularly to non-Governmental customers, and are provided by the offeror (or subcontractor in the case of an exempt subcontract) to the general public in substantial quantities in the course of normal business operations;

(ii) The contract services will be furnished at prices that are, or are based on, established catalog or market prices (see FAR 22.1003-4(d)(2)(iii));

(iii) Each service employee who will perform the services under the contract will spend only a small portion of his or her time (a monthly average of less than 20 percent of the available hours on an annualized basis, or less than 20 percent of available hours during the contract period if the contract period is less than a month) servicing the Government contract; and

(iv) The compensation (wage and fringe benefits) plan for all service employees performing work under the contract is the same as that used for these employees and equivalent employees servicing commercial customers.

(3) If paragraph (k)(1) or (k)(2) of this clause applies—

(i) If the offeror does not certify to the conditions in paragraph (k)(1) or (k)(2) and the Contracting Officer did not attach a Service Contract Labor Standards wage determination to the solicitation, the offeror shall notify the Contracting Officer as soon as possible; and

(ii) The Contracting Officer may not make an award to the offeror if the offeror fails to execute the certification in paragraph (k)(1) or (k)(2) of this clause or to contact the Contracting Officer as required in paragraph (k)(3)(i) of this clause.

(l) *Taxpayer Identification Number (TIN) (26 U.S.C. 6109, 31 U.S.C. 7701)*. (Not applicable if the offeror is required to provide this information to the SAM database to be eligible for award.)

(1) All offerors must submit the information required in paragraphs (l)(3) through (l)(5) of this provision to comply with debt collection requirements of 31 U.S.C. 7701(c) and 3325(d), reporting requirements of 26 U.S.C. 6041, 6041A, and 6050M, and implementing regulations issued by the Internal Revenue Service (IRS).

(2) The TIN may be used by the Government to collect and report on any delinquent amounts arising out of the offeror's relationship with the Government (31 U.S.C. 7701(c)(3)). If the resulting contract is subject to the payment reporting requirements described in FAR 4.904, the TIN provided hereunder may be matched with IRS records to verify the accuracy of the offeror's TIN.

(3) *Taxpayer Identification Number* (TIN).

**[ ]** TIN:_____

**[ ]** TIN has been applied for.

**[ ]** TIN is not required because:

**[ ]** Offeror is a nonresident alien, foreign corporation, or foreign partnership that does not have income effectively connected with the conduct of a trade or business in the United States and does not have an office or place of business or a fiscal paying agent in the United States;

**[ ]** Offeror is an agency or instrumentality of a foreign government;

**[ ]** Offeror is an agency or instrumentality of the Federal Government.

(4) *Type of organization.*

**[ ]** Sole proprietorship;

**[ ]** Partnership;

**[ ]** Corporate entity (not tax-exempt);

**[ ]** Corporate entity (tax-exempt);

**[ ]** Government entity (Federal, State, or Local);

**[ ]** Foreign government;

**[ ]** International organization per 26 CFR 1.6049-4;

**[ ]** Other_____

(5) *Common parent.*

**[ ]** Offeror is not owned or controlled by a common parent;

**[ ]** Name and TIN of common parent:

Name_____

TIN_____

(m) *Restricted business operations in Sudan*. By submission of its offer, the offeror certifies that the offeror does not conduct any restricted business operations in Sudan.

(n) *Prohibition on Contracting with Inverted Domestic Corporations.*

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

(2) *Representation*. By submission of its offer, the offeror represents that—

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

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

(o) *Prohibition on contracting with entities engaging in certain activities or transactions relating to Iran*.

(1) The offeror shall email questions concerning sensitive technology to the Department of State at CISADA106@state.gov.

(2) Representation and Certification. Unless a waiver is granted or an exception applies as provided in paragraph (o)(3) of this provision, by submission of its offer, the offeror—

(i) Represents, to the best of its knowledge and belief, that the offeror does not export any sensitive technology to the government of Iran or any entities or individuals owned or controlled by, or acting on behalf or at the direction of, the government of Iran;

(ii) Certifies that the offeror, or any person owned or controlled by the offeror, does not engage in any activities for which sanctions may be imposed under section 5 of the Iran Sanctions Act; and

(iii) Certifies that the offeror, and any person owned or controlled by the offeror, does not knowingly engage in any transaction that exceeds $3,500 with Iran's Revolutionary Guard Corps or any of its officials, agents, or affiliates, the property and interests in property of which are blocked pursuant to the International Emergency Economic Powers Act (50(U.S.C. 1701 et seq.) (see OFAC's Specially Designated Nationals and Blocked Persons List at http://www.treasury.gov/ofac/downloads/t11sdn.pdf ).

(3) The representation and certification requirements of paragraph (o)(2) of this provision do not apply if—

(i) This solicitation includes a trade agreements certification (e.g., 52.212-3(g) or a comparable agency provision); and

(ii) The offeror has certified that all the offered products to be supplied are designated country end products.

(p) *Ownership or Control of Offeror*. (Applies in all solicitations when there is a requirement to be registered in SAM or a requirement to have a unique entity identifier in the solicitation.

(1) The Offeror represents that it [ ] has or [ ] does not have an immediate owner. If the Offeror has more than one immediate owner (such as a joint venture), then the Offeror shall respond to paragraph (2) and if applicable, paragraph (3) of this provision for each participant in the joint venture.

(2) If the Offeror indicates "has" in paragraph (p)(1) of this provision, enter the following information:

Immediate owner CAGE code:_____

Immediate owner legal name:_____

(Do not use a "doing business as" name)

Is the immediate owner owned or controlled by another entity:

**[ ]** Yes or **[ ]** No.

(3) If the Offeror indicates "yes" in paragraph (p)(2) of this provision, indicating that the immediate owner is owned or controlled by another entity, then enter the following information:

Highest level owner CAGE code:_____

Highest level owner legal name:_____

(Do not use a "doing business as" name)

(q) *Representation by Corporations Regarding Delinquent Tax Liability or a Felony Conviction under any Federal Law.*

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

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

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

(2) The Offeror represents that--

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

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

(r) *Predecessor of Offeror.* (Applies in all solicitations that include the provision at 52.204-16, Commercial and Government Entity Code Reporting.)

(1) The Offeror represents that it **[ ] is** or **[ ] is not** a successor to a predecessor that held a Federal contract or grant within the last three years.

(2) If the Offeror has indicated "is" in paragraph (r)(1) of this provision, enter the following information for all predecessors that held a Federal contract or grant within the last three years (if more than one predecessor, list in reverse chronological order):

Predecessor CAGE code _____(or mark "Unknown).

Predecessor legal name: _____.
(Do not use a "doing business as" name).

(s) [Reserved].

(t) Public Disclosure of Greenhouse Gas Emissions and Reduction Goals. Applies in all solicitations that require offerors to register in SAM (52.212-1(k)).

(1) This representation shall be completed if the Offeror received $7.5 million or more in contract awards in the prior Federal fiscal year. The representation is optional if the Offeror received less than $7.5 million in Federal contract awards in the prior Federal fiscal year.

(2) Representation. [Offeror to check applicable block(s) in paragraph (t)(2)(i) and (ii)].

(i) The Offeror (itself or through its immediate owner or highest-level owner) **[ ] does, [ ] does not** publicly disclose greenhouse gas emissions, i.e., makes available on a publicly accessible Web site the results of a greenhouse gas inventory, performed in accordance with an accounting standard with publicly available and consistently applied criteria, such as the Greenhouse Gas Protocol Corporate Standard.

(ii) The Offeror (itself or through its immediate owner or highest-level owner) **[ ] does, [ ] does not** publicly disclose a quantitative greenhouse gas emissions reduction goal, i.e., make available on a publicly accessible Web site a target to reduce absolute emissions or emissions intensity by a specific quantity or percentage.

(iii) A publicly accessible Web site includes the Offeror's own Web site or a recognized, third-party greenhouse gas emissions reporting program.

(3) If the Offeror checked “does” in paragraphs (t)(2)(i) or (t)(2)(ii) of this provision, respectively, the Offeror shall provide the publicly accessible Web site(s) where greenhouse gas emissions and/or reduction goals are reported:_____.

**(End of provision)**

**52.212-5 CONTRACT TERMS AND CONDITIONS REQUIRED TO IMPLEMENT STATUTES OR EXECUTIVE ORDERS--COMMERCIAL ITEMS (JAN 2018)**

(a) The Contractor shall comply with the following Federal Acquisition Regulation (FAR) clauses, which are incorporated in this contract by reference, to implement provisions of law or Executive orders applicable to acquisitions of commercial items:

(1) **52.203-19**, Prohibition on Requiring Certain Internal Confidentiality Agreements or Statements (JAN 2017) (section 743 of Division E, Title VII, of the Consolidated and Further Continuing Appropriations Act, 2015 (Pub. L.

113-235) and its successor provisions in subsequent appropriations acts (and as extended in continuing resolutions)).

(2) **52.209-10,** Prohibition on Contracting with Inverted Domestic Corporations (Nov 2015).

(3) **52.233-3**, Protest After Award (Aug 1996)(31 U.S.C 3553).

(4) **52.233-4**, Applicable Law for Breach of Contract Claim (Oct 2004)(Public Laws 108-77 and 108-78 (19 U.S.C. 3805 note)).

(b) The Contractor shall comply with the FAR clauses in this paragraph (b) that the Contracting Officer has indicated as being incorporated in this contract by reference to implement provisions of law or Executive orders applicable to acquisitions of commercial items:

*[Contracting Officer check as appropriate.]*

__X__ (1) **52.203-6**, Restrictions on Subcontractor Sales to the Government (Sep 2006), with **Alternate I** (Oct 1995)(41 U.S.C. 4704 and 10 U.S.C. 2402).

__X__ (2) **52.203-13,** Contractor Code of Business Ethics and Conduct (Oct 2015) (41 U.S.C. 3509).

__-__ (3) **52.203-15**, Whistleblower Protections Under the American Recovery and Reinvestment Act of 2009 (Jun 2010) (Section 1553 of Pub. L. 111-5). (Applies to contracts funded by the American Recovery and Reinvestment Act of 2009.)

__X__ (4) **52.204-10**, Reporting Executive Compensation and First-Tier Subcontract Awards (Oct 2016) (Pub. L. 109-282) (31 U.S.C. 6101 note).

(5) [Reserved]

__-__ (6) **52.204-14**, Service Contract Reporting Requirements (Oct 2016) (Pub. L. 111-117, section 743 of Div. C).

__X__ (7) **52.204-15,** Service Contract Reporting Requirements for Indefinite-Delivery Contracts (Oct 2016) (Pub. L. 111-117, section 743 of Div. C).

__X__ (8) **52.209-6**, Protecting the Government's Interest When Subcontracting with Contractors Debarred, Suspended, or Proposed for Debarment (Oct 2015) (31 U.S.C. 6101 note).

__X__ (9) **52.209-9,** Updates of Publicly Available Information Regarding Responsibility Matters (Jul 2013) (41 U.S.C. 2313).

(10) [Reserved]

__X__ (11) (i) **52.219-3**, Notice of HUBZone Set-Aside or Sole-Source Award (Nov 2011)(15 U.S.C. 657a).

__-__ (ii) **Alternate I** (Nov 2011) of 52.219-3.

__-__ (12) (i) **52.219-4**, Notice of Price Evaluation Preference for HUBZone Small Business Concerns (Oct 2014) (if the offeror elects to waive the preference, it shall so indicate in its offer)(15 U.S.C. 657a).

__-__ (ii) **Alternate I** (Jan 2011) of 52.219-4.

(13) [Reserved]

__X__ (14) (i) **52.219-6**, Notice of Total Small Business Set-Aside (Nov 2011)(15 U.S.C. 644).

__-__ (ii) **Alternate I** (Nov 2011).

__-__ (iii) **Alternate II** (Nov 2011).

__-__ (15) (i) **52.219-7**, Notice of Partial Small Business Set-Aside (June 2003)(15 U.S.C. 644).

__-__ (ii) **Alternate I** (Oct 1995) of 52.219-7.

__-__ (iii) **Alternate II** (Mar 2004) of 52.219-7.

__X__ (16) **52.219-8**, Utilization of Small Business Concerns (Nov 2016) (15 U.S.C. 637(d)(2) and (3)).

__-__ (17) (i) **52.219-9**, Small Business Subcontracting Plan (Nov 2016) (15 U.S.C. 637(d)(4)). (In accordance with DPAP Memo dated 15 Aug 2016, DAR Tracking Number

2016-O0009, Class Deviation—Subcontract Reporting, this clause and any applicable alternates are replaced with DFARS Deviation(s) dated Aug 2016, listed below when applicable. Effective until incorporated into the FAR or DFARS or until rescinded.)

__-__ (ii) **Alternate I** (Nov 2016) of 52.219-9.

__-__ (iii) **Alternate II** (Nov 2016) of 52.219-9.

__-__ (iv) **Alternate III** (Nov 2016) of 52.219-9.

____ (v) **Alternate IV** (Nov 2016) of 52.219-9.

____ (18) **52.219-13**, Notice of Set-Aside of Orders (Nov 2011) (15 U.S.C. 644(r)).

_X_- (19) **52.219-14**, Limitations on Subcontracting (Jan 2017)(15 U.S.C. 637(a)(14)).

__-__ (20) **52.219-16**, Liquidated Damages—Subcontracting Plan (Jan 1999) (15 U.S.C. 637(d)(4)(F)(i)).

__-__ (21) **52.219-27**, Notice of Total Service-Disabled Veteran-Owned Small Business Set-Aside (Nov 2011)(15 U.S.C. 657 f).

__**X**__ (22) **52.219-28**, Post Award Small Business Program Representation (Jul 2013) (15 U.S.C. 632(a)(2)).

__-__ (23) **52.219-29,** Notice of Set-Aside for, or Sole source Award to, Economically Disadvantaged Women-Owned Small Business Concerns (Dec 2015) (1 U.S.C. 637(m)).

__-__ (24) **52.219-30,** Notice of Set-Aside for, or Sole source Award to, Women-Owned Small Business Concerns Eligible Under the Women-Owned Small Business Program (Dec 2015) (15 U.S.C. 637(m)).

__**X**__ (25) **52.222-3**, Convict Labor (June 2003)(E.O. 11755).

__-__ (26) **52.222-19**, Child Labor—Cooperation with Authorities and Remedies (Jan 2018) (E.O. 13126).

__**X**__ (27) **52.222-21**, Prohibition of Segregated Facilities (Apr 2015).

__X__ (28) **52.222-26**, Equal Opportunity (Sept 2016)(E.O. 11246).

__X__ (29) **52.222-35**, Equal Opportunity for Veterans (Oct 2015)(38 U.S.C. 4212).

__X__ (30) **52.222-36**, Equal Opportunity For Workers with Disabilities (Jul 2014)(29 U.S.C. 793).

__X__ (31) **52.222-37**, Employment Reports on Veterans (Feb 2016)(38 U.S.C. 4212).

__X__ (32) **52.222-40**, Notification of Employee Rights Under the National Labor relations Act (Dec 2010) E.O. 13496).

__X__ (33) (i) **52.222-50**, Combating Trafficking in Persons (Mar 2015) (22 U.S.C. chapter 78 and E.O. 13627).

__-__ (ii) **Alternate I** (Mar 2015) of 52.222-50 (22 U.S.C. chapter 78 and E.O. 13627).

_X__ (34) **52.222-54**, Employment Eligibility Verification (Oct 2015). (E. O. 12989). (Not applicable to the acquisition of commercially available off-the-shelf items or certain other types of commercial items as prescribed in 22.1803.)

__-__ (35) (i) **52.223-9**, Estimate of Percentage of Recovered Material Content for EPA-Designated Items (May 2008)(42 U.S.C. 6962(c)(3)(A)(ii)). (Not applicable to the acquisition of commercially available off-the-shelf items.)

__-_ (ii) **Alternate I** (May 2008) of 52.223-9 (42 U.S.C. 6962(i)(2)(C)). (Not applicable to the acquisition of commercially available off-the-shelf items.)

__-__ (36) **52.223-11**, Ozone-Depleting Substances and High Global Warming Potential Hydrofluorocarbons (June 2016) (E.O. 13693).

__-__ (37) **52.223-12**, Maintenance, Service, repair, or Disposal of Refrigeration Equipment and Air Conditioners (June 2016) (E.O.13693).

___ (38) (i) **52.223-13**, Acquisition of EPEAT®-Registered Imaging Equipment (Jun 2014) (E.O.s 13423 and 13514).

___ (ii) **Alternate I** (Oct 2015) of 52.223-13.

___ (39) (i) **52.223-14**, Acquisition of EPEAT®-Registered Televisions (Jun 2014) (E.O.s 13423 and 13514).

___ (ii) **Alternate I** (Jun 2014) of 52.223-14.

___ (40) **52.223-15**, Energy Efficiency in Energy-Consuming Products (Dec 2007) (42.U.S.C. 8259b).

___ (41) (i) **52.223-16**, Acquisition of EPEAT®-Registered Personal Computer Products (Oct 2015) (E.O.s 13423 and 13514).

___ (ii) **Alternate I** (Oct 2015) of 52.223-16.

__X__ (42) **52.223-18**, Encouraging Contractor Policies to Ban Text Messaging While Driving (Aug 2011) (E.O.13513).

___ (43) **52.223-20**, Aerosols (June 2016) (E.O. 13693)

___ (44) **52.223-21**, Foams (June 2016) (E.O. 13693).

__X___ (45) (i) **52.224-3**, Privacy Training (JAN 2017) (5 U.S.C. 552a).

___ (ii) Alternate I (JAN 2017) of 52.224-3.

___ (46) **52.225-1**, Buy American--Supplies (May 2014) (41 U.S.C. chapter 83).

___ (47) (i) **52.225-3**, Buy American--Free Trade Agreements--Israeli Trade Act (May 2014) (41 U.S.C. chapter 83, 19 U.S.C. 3301 note, 19 U.S.C. 2112 note, 19 U.S.C. 3805 note, 19 U.S.C. 4001 note, Pub. L. 103-182, 108-77, 108-78, 108-286, 108-302, 109-53, 109-169, 109-283, 110-138, 112-41, 112-42, and 112-43).

___ (ii) **Alternate I** (May 2014) of 52.225-3.

___ (iii) **Alternate II** (May 2014) of 52.225-3.

___ (iv) **Alternate III** (May 2014) of 52.225-3.

__-__ (48) **52.225-5**, Trade Agreements (Oct 2016) (19 U.S.C. 2501, *et seq.*, 19 U.S.C. 3301 note).

__**X**__ (49) **52.225-13**, Restriction on Certain Foreign Purchases (Jun 2008)(E.O.s, proclamations, and statutes administered by the Office of Foreign Assets Control of the Department of Treasury).

__-__ (50) **52.225-26**, Contractors Performing Private Security Functions Outside the United States (Oct 2016) (Section 862, as amended, of the National Defense Authorization Act for Fiscal Year 2008; 10 U.S.C. 2302 Note).

__-__ (51) **52.226-4**, Notice of Disaster or Emergency Area Set-Aside (Nov 2007)(42 U.S.C. 5150).

__-__ (52) **52.226-5**, Restrictions on Subcontracting Outside Disaster or Emergency Area (Nov 2007)(42 U.S.C. 5150).

__-__ (53) **52.232-29**, Terms for financing of Purchases of Commercial Items (Feb 2002)(41 U.S.C. 4505, 10 U.S.C. 2307(f)).

__-__ (54) **52.232-30**, Installment Payments for Commercial Items (Oct 1995)(41 U.S.C. 4505, 10 U.S.C. 2307(f)).

__X__ (55) **52.232-33**, Payment by Electronic Funds Transfer—System for Award Management (Jul 2013)(31.U.S.C. 3332).

__-__ (56) **52.232-34**, Payment by Electronic Funds Transfer—Other than System for Award Management (Jul 2013)(31.U.S.C. 3332).

__-__ (57) **52.232-36**, Payment by Third Party (May 2014) (31 U.S.C. 3332).

__-__ (58) **52.239-1**, Privacy or Security Safeguards (Aug 1996)(5 U.S.C. 552a).

_X__ (59) **52.242-5**, Payments to Small Business Subcontractors (JAN 2017)(15 U.S.C. 637(d)(12)).

__-__ (i) **52.247-64**, Preference for Privately Owned U.S.-Flag Commercial Vessels (Feb 2006) (46 U.S.C. Appx. 1241(b) and 10 U.S.C. 2631).

__-__ (ii) **Alternate I** (Apr 2003) of 52.247-64.

(c) The Contractor shall comply with the FAR clauses in this paragraph (c), applicable to commercial services, that the Contracting Officer has indicated as being incorporated in this contract by reference to implement provisions of law or Executive orders applicable to acquisitions of commercial items:

*[Contracting Officer check as appropriate.]*

__X__ (1) **52.222-17**, Nondisplacement of Qualified Workers (May 2014) (E.O. 13495).

__X__ (2) **52.222-41**, Service Contract Labor Standards (May 2014) (41 U.S.C. chapter 67).

__X__ (3) **52.222-42**, Statement of Equivalent Rates for Federal Hires (May 2014) (29 U.S.C. 206 and 41 U.S.C. chapter 67).

__X__ (4) **52.222-43**, Fair Labor Standards Act and Service Contract Labor Standards--Price Adjustment (Multiple Year and Option Contracts) (May 2014)(29 U.S.C. 206 and 41 U.S.C. chapter 67).

__X__ (5) **52.222-44**, Fair Labor Standards Act and Service Contract Labor Standards - Price Adjustment (May 2014) (29 U.S.C. 206 and 41 U.S.C. chapter 67).

__-__ (6) **52.222-51**, Exemption from Application of the Service Contract Labor Standards to Contracts for Maintenance, Calibration, or Repair of Certain Equipment—Requirements (May 2014) (41 U.S.C. chapter 67).

__-__ (7) **52.222-53**, Exemption from Application of the Service Contract Labor Standards to Contracts for Certain Services—Requirements (May 2014)(41 U.S.C. chapter 67).

__X__ (8) **52.222-55**, Minimum Wages Under Executive Order 13658 (Dec 2015).

__X__ (9) **52.222-62**, Paid Sick Leave Under Executive Order 13706.

(JAN 2016) (E.O. 13706).

___ (10) **52.226-6**, Promoting Excess Food Donation to Nonprofit Organizations. (May 2014) (42 U.S.C. 1792).

___ (11) **52.237-11**, Accepting and Dispensing of $1 Coin (Sep 2008) (31 U.S.C. 5112(p)(1)).

(d) *Comptroller General Examination of Record*. The Contractor shall comply with the provisions of this paragraph (d) if this contract was awarded using other than sealed bid, is in excess of the simplified acquisition threshold, and does not contain the clause at 52.215-2, Audit and Records--Negotiation.

(1) The Comptroller General of the United States, or an authorized representative of the Comptroller General, shall have access to and right to examine any of the Contractor's directly pertinent records involving transactions related to this contract.

(2) The Contractor shall make available at its offices at all reasonable times the records, materials, and other evidence for examination, audit, or reproduction, until 3 years after final payment under this contract or for any shorter period specified in FAR Subpart 4.7, Contractor Records Retention, of the other clauses of this contract. If this contract is completely or partially terminated, the records relating to the work terminated shall be made available for 3 years after any resulting final termination settlement. Records relating to appeals under the disputes clause or to litigation or the settlement of claims arising under or relating to this contract shall be made available until such appeals, litigation, or claims are finally resolved.

(3) As used in this clause, records include books, documents, accounting procedures and practices, and other data, regardless of type and regardless of form. This does not require the Contractor to create or maintain any record that the Contractor does not maintain in the ordinary course of business or pursuant to a provision of law.

(e)(1) Notwithstanding the requirements of the clauses in paragraphs (a), (b), (c) and (d) of this clause, the Contractor is not required to flow down any FAR clause, other than those in paragraphs (e)(1) of this paragraph in a subcontract for commercial items. Unless otherwise indicated below, the extent of the flow down shall be as required by the clause—

(i) **52.203-13**, Contractor Code of Business Ethics and Conduct (Oct 2015) (41 U.S.C. 3509).

(ii) **52.203-19**, Prohibition on Requiring Certain Internal Confidentiality Agreements or Statements (Jan 2017) (section 743 of Division E, Title VII, of the Consolidated and Further Continuing Appropriations Act, 2015 (Pub. L.

113-235) and its successor provisions in subsequent appropriations acts (and as extended in continuing resolutions)).

(iii) **52.219-8**, Utilization of Small Business Concerns (Nov 2016) (15 U.S.C. 637(d)(2) and (3)), in all subcontracts that offer further subcontracting opportunities. If the subcontract (except subcontracts to small business concerns) exceeds $700,000 ($1.5 million for construction of any public facility), the subcontractor must include 52.219-8 in lower tier subcontracts that offer subcontracting opportunities.

(iv) **52.222-17**, Nondisplacement of Qualified Workers (May 2014) (E.O. 13495). Flow Down required in accordance with paragraph (l) of FAR clause 52.222-17.

(v) **52.222-21**, Prohibition of Segregated Facilities (Apr 2015).

(vi) **52.222-26**, Equal Opportunity (Sept 2016) (E.O. 11246).

(vii) **52.222-35**, Equal Opportunity for Veterans (Oct 2015) (38 U.S.C. 4212).

(viii) **52.222-36**, Equal Opportunity for Workers with Disabilities (Jul 2014) (29 U.S.C. 793).

(ix) **52.222-37**, Employment Reports on Veterans (Feb 2016) (38 U.S.C. 4212).

(x) **52.222-40**, Notification of Employee Rights Under the National Labor Relations Act (Dec 2010) (E.O. 13496). Flow down required in accordance with paragraph (f) of FAR clause 52.222-40.

(xi) **52.222-41**, Service Contract Labor Standards (May 2014) (41 U.S.C. chapter 67).

(xii) __**X**__ (A) **52.222-50**, Combating Trafficking in Persons (Mar 2015) (22 U.S.C. chapter 78 and E.O. 13627).

___(B) **Alternate I** (Mar 2015) of 52.222-50 (22 U.S.C. chapter 78 and E.O. 13627).

(xiii) **52.222-51**, Exemption from Application of the Service Contract Labor Standards to Contracts for Maintenance, Calibration, or Repair of Certain Equipment—Requirements (May 2014) (41 U.S.C. chapter 67).

(xiv) **52.222-53**, Exemption from Application of the Service Contract Labor Standards to Contracts for Certain Services—Requirements (May 2014) (41 U.S.C. chapter 67).

(xv) **52.222-54,** Employment Eligibility Verification (Oct 2015) (E. O. 12989).

(xvi) **52.222-55,** Minimum Wages Under Executive Order 13658 (Dec 2015).

(xvii) **52.222-62**, Paid Sick Leave Under Executive Order 13706 (JAN 2017) (E.O. 13706).

(xviii)(A) 52.224-3, Privacy Training (JAN 2017) (5 U.S.C. 552a).
(B) Alternate I (JAN 2017) of 52.224-3.

(xix) **52.225-26,** Contractors Performing Private Security Functions Outside the United States (Oct 2016) (Section 862, as amended, of the National Defense Authorization Act for Fiscal Year 2008; 10 U.S.C. 2302 Note).

(xx) **52.226-6**, Promoting Excess Food Donation to Nonprofit Organizations (May 2014) (42 U.S.C. 1792). Flow down required in accordance with paragraphs (e) of FAR clause 52.226-6.

(xxi) **52.247-64**, Preference for Privately Owned U.S.-Flag Commercial Vessels (Feb 2006) (46 U.S.C. Appx 1241(b) and 10 U.S.C. 2631). Flow down required in accordance with paragraph (d) of FAR clause 52.247-64.

(2) While not required, the Contractor may include in its subcontracts for commercial items a minimal number of additional clauses necessary to satisfy its contractual obligations.

**(End of clause)**

**52.217-8 Option to Extend Services (NOV 1999)**

The Government may require continued performance of any services within the limits and at the rates specified in the contract. These rates may be adjusted only as a result of revisions to prevailing labor rates provided by the Secretary of Labor. The option provision may be exercised more than once, but the total extension of performance hereunder shall not exceed 6 months. The Contracting Officer may exercise the option by written notice to the Contractor within 60 calendar days.

**(End of clause)**

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

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

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

(c) The total duration of this contract, including the exercise of any options under this clause, shall not exceed five (5) years.

**(End of clause)**

**52.222-54 Employment Eligibility Verification (OCT 2015)**

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

"Commercially available off-the-shelf (COTS) item"—

(1) Means any item of supply that is—

(i) A commercial item (as defined in paragraph (1) of the definition at 2.101);

(ii) Sold in substantial quantities in the commercial marketplace; and

(iii) Offered to the Government, without modification, in the same form in which it is sold in the commercial marketplace; and

(2) Does not include bulk cargo, as defined in 46 U.S.C. 40102(4), such as agricultural products and petroleum products. Per 46 CFR 525.1 (c)(2), "bulk cargo" means cargo that is loaded and carried in bulk onboard ship without mark or count, in a loose unpackaged form, having homogenous characteristics. Bulk cargo loaded into intermodal equipment, except LASH or Seabee barges, is subject to mark and count and, therefore, ceases to be bulk cargo.

"Employee assigned to the contract" means an employee who was hired after November 6, 1986, (after November 27, 2009 in the Commonwealth of the Northern Mariana Islands), who is directly performing work, in the United States, under a contract that is required to include the clause prescribed at 22.1803. An employee is not considered to be directly performing work under a contract if the employee—

(1) Normally performs support work, such as indirect or overhead functions; and

(2) Does not perform any substantial duties applicable to the contract.

"Subcontract" means any contract, as defined in 2.101, entered into by a subcontractor to furnish supplies or services for performance of a prime contract or a subcontract. It includes but is not limited to purchase orders, and changes and modifications to purchase orders.

"Subcontractor" means any supplier, distributor, vendor, or firm that furnishes supplies or services to or for a prime Contractor or another subcontractor.

"United States", as defined in 8 U.S.C. 1101(a)(38), means the 50 States, the District of Columbia, Puerto Rico, Guam, the Commonwealth of the Northern Mariana Islands, and the U.S. Virgin Islands.

(b) *Enrollment and verification requirements*.

(1) If the Contractor is not enrolled as a Federal Contractor in E-Verify at time of contract award, the Contractor shall—

(i) *Enroll*. Enroll as a Federal Contractor in the E-Verify program within 30 calendar days of contract award;

(ii) *Verify all new employees*. Within 90 calendar days of enrollment in the E-Verify program, begin to use E-Verify to initiate verification of employment eligibility of all new hires of the Contractor, who are working in the United States, whether or not assigned to the contract, within 3 business days after the date of hire (but see paragraph (b)(3) of this section); and

(iii) *Verify employees assigned to the contract*. For each employee assigned to the contract, initiate verification within 90 calendar days after date of enrollment or within 30 calendar days of the employee's assignment to the contract, whichever date is later (but see paragraph (b)(4) of this section).

(2) If the Contractor is enrolled as a Federal Contractor in E-Verify at time of contract award, the Contractor shall use E-Verify to initiate verification of employment eligibility of—

(i) *All new employees*.

(A) *Enrolled 90 calendar days or more*. The Contractor shall initiate verification of all new hires of the Contractor, who are working in the United States, whether or not assigned to the contract, within 3 business days after the date of hire (but see paragraph (b)(3) of this section); or

(B) *Enrolled less than 90 calendar days*. Within 90 calendar days after enrollment as a Federal Contractor in E-Verify, the Contractor shall initiate verification of all new hires of the Contractor, who are working in the United States, whether or not assigned to the contract, within 3 business days after the date of hire (but see paragraph (b)(3) of this section); or

(ii) *Employees assigned to the contract*. For each employee assigned to the contract, the Contractor shall initiate verification within 90 calendar days after date of contract award or within 30 days after assignment to the contract, whichever date is later (but see paragraph (b)(4) of this section).

(3) If the Contractor is an institution of higher education (as defined at 20 U.S.C. 1001(a)); a State or local government or the government of a Federally recognized Indian tribe; or a surety performing under a takeover agreement entered into with a Federal agency pursuant to a performance bond, the Contractor may choose to verify only employees assigned to the contract, whether existing employees or new hires. The Contractor shall follow the applicable verification requirements at (b)(1) or (b)(2) respectively, except that any requirement for verification of new employees applies only to new employees assigned to the contract.

(4) *Option to verify employment eligibility of all employees*. The Contractor may elect to verify all existing employees hired after November 6, 1986 (after November 27, 2009, in the Commonwealth of the Northern Mariana Islands), rather than just those employees assigned to the contract. The Contractor shall initiate verification for each existing employee working in the United States who was hired after November 6, 1986 (after November 27, 2009, in the Commonwealth of the Northern Mariana Islands), within 180 calendar days of—

(i) Enrollment in the E-Verify program; or

(ii) Notification to E-Verify Operations of the Contractor's decision to exercise this option, using the contact information provided in the E-Verify program Memorandum of Understanding (MOU).

(5) The Contractor shall comply, for the period of performance of this contract, with the requirements of the E-Verify program MOU.

(i) The Department of Homeland Security (DHS) or the Social Security Administration (SSA) may terminate the Contractor's MOU and deny access to the E-Verify system in accordance with the terms of the MOU. In such case, the Contractor will be referred to a suspension or debarment official.

(ii) During the period between termination of the MOU and a decision by the suspension or debarment official whether to suspend or debar, the Contractor is excused from its obligations under paragraph (b) of this clause. If the suspension or debarment official determines not to suspend or debar the Contractor, then the Contractor must reenroll in E-Verify.

(c) *Web site*. Information on registration for and use of the E-Verify program can be obtained via the Internet at the Department of Homeland Security Web site: *http://www.dhs.gov/E-Verify*.

(d) *Individuals previously verified*. The Contractor is not required by this clause to perform additional employment verification using E-Verify for any employee—

(1) Whose employment eligibility was previously verified by the Contractor through the E-Verify program;

(2) Who has been granted and holds an active U.S. Government security clearance for access to confidential, secret, or top secret information in accordance with the National Industrial Security Program Operating Manual; or

(3) Who has undergone a completed background investigation and been issued credentials pursuant to Homeland Security Presidential Directive (HSPD)-12, Policy for a Common Identification Standard for Federal Employees and Contractors.

(e) *Subcontracts*. The Contractor shall include the requirements of this clause, including this paragraph (e) (appropriately modified for identification of the parties), in each subcontract that—

(1) Is for—

(i) Commercial or noncommercial services (except for commercial services that are part of the purchase of a COTS item (or an item that would be a COTS item, but for minor modifications), performed by the COTS provider, and are normally provided for that COTS item); or

(ii) Construction;

(2) Has a value of more than $3,500; and

(3) Includes work performed in the United States.

**(End of clause)**

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

(a) Upon receipt of accelerated payments from the Government, the Contractor shall make accelerated payments to its small business subcontractors under this contract, to the maximum extent practicable and prior to when such payment is otherwise required under the applicable contract or subcontract, after receipt of a proper invoice and all other required documentation from the small business subcontractor.

(b) The acceleration of payments under this clause does not provide any new rights under the Prompt Payment Act.

(c) Include the substance of this clause, including this paragraph (c), in all subcontracts with small business concerns, including subcontracts with small business concerns for the acquisition of commercial items.

**(End of clause)**

**52.252-1 Solicitation Provisions Incorporated by Reference (FEB 1998)**

This solicitation incorporates one or more solicitation provisions 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. The offeror is cautioned that the listed provisions may include blocks that must be completed by the offeror and submitted with its quotation or offer. In lieu of submitting the full text of those provisions, the offeror may identify the provision by paragraph identifier and provide the appropriate information with its quotation or offer. Also, the full text of a solicitation provision may be accessed electronically at this/these address(es):

http://farsite.hill.af.mil/farsite.html
http://farsite.hill.af.mil/VFHSARA.HTM

**(End of provision)**

**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):

http://farsite.hill.af.mil/farsite.html
http://farsite.hill.af.mil/VFHSARA.HTM

**(End of clause)**

**52.252-5 Authorized Deviations in Provisions (APR 1984)**

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

(b) The use in this solicitation of any Department of Homeland Security (48 CFR Chapter 30) provision with an authorized deviation is indicated by the addition of "(DEVIATION)" after the name of the regulation.

**(End of provision)**

**52.252-6 Authorized Deviations in Clauses.**

As prescribed in 52.107(f), insert the following clause in solicitations and contracts that include any FAR or supplemental clause with an authorized deviation. Whenever any FAR or supplemental clause is used with an authorized deviation, the contracting officer shall identify it by the same number, title, and date assigned to the clause when it is used without deviation, include regulation name for any supplemental clause, except that the contracting officer shall insert "(Deviation)" after the date of the clause.

**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 Department of Homeland Security (48 CFR Chapter 30) clause with an authorized deviation is indicated by the addition of "(DEVIATION)" after the name of the regulation.

**(End of clause)**

**HOMELAND SECURITY ACQUISITION REGULATION (CFR CHAPTER 30 CLAUSES) CLAUSES INCORPORATED BY REFERENCE**

This section contains clauses, which are incorporated by reference, with the same force and effect as if they were in full text. Upon request, the Contract Specialist will make their full text available.

| CLAUSE NO. | CLAUSE TITLE | DATE |
|---|---|---|

| | | |
|---|---|---|
| 3052.209-70 | Prohibition on Contract with Corporate Expatriates | JUN 2006 |
| 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 |
| 3052.222-90 | Local Hire (USCG) | JUN 2006 |
| 3052-223-90 | Accident and Fire Reporting (USCG) | DEC 2003 |

**HOMELAND SECURITY ACQUISITION REGULATION CLAUSES INCORPORATED BY FULL TEXT**

**3052.212-70 Contract Terms and Conditions Applicable to DHS Acquisition of Commercial Items.**

**CONTRACT TERMS AND CONDITIONS APPLICABLE TO DHS ACQUISITION OF COMMERCIAL ITEMS (SEP 2012)**

The Contractor agrees to comply with any provision or clause that is incorporated herein by reference to implement agency policy applicable to acquisition of commercial items or components. The provision or clause in effect based on the applicable regulation cited on the date the solicitation is issued applies unless otherwise stated herein. The following provisions and clauses marked with an "X" are incorporated by reference:

(a) Provisions.

_X_3052.209-72 Organizational Conflicts of Interest.

____3052.216-70 Evaluation of Offers Subject to An Economic Price Adjustment Clause.

____3052.219-72 Evaluation of Prime Contractor Participation in the DHS Mentor Protégé Program.

(b) Clauses.

_X_3052.203-70 Instructions for Contractor Disclosure of Violations.

____3052.204-70 Security Requirements for Unclassified Information Technology Resources.

_X_3052.204-71 Contractor Employee Access.

_X_Alternate I

_X_3052.205-70 Advertisement, Publicizing Awards, and Releases.

_X_3052.209-73 Limitation on Future Contracting.

__X__ 3052.215-70 Key Personnel or Facilities.

____3052.216-71 Determination of Award Fee.

____3052.216-72 Performance Evaluation Plan.

____3052.216-73 Distribution of Award Fee.

____3052.217-91 Performance. (USCG)

____3052.217-92 Inspection and Manner of Doing Work. (USCG)

____3052.217-93 Subcontracts. (USCG)

____3052.217-94 Lay Days. (USCG)

____3052.217-95 Liability and Insurance. (USCG)

____3052.217-96 Title. (USCG)

____3052.217-97 Discharge of Liens. (USCG)

____3052.217-98 Delays. (USCG)

____3052.217-99 Department of Labor Safety and Health Regulations for Ship Repair. (USCG)

____3052.217-100 Guarantee. (USCG)

____3052.219-70 Small Business Subcontracting Plan Reporting.

____3052.219-71 DHS Mentor Protégé Program.

__X__3052.228-70 Insurance.

____3052.228-90 Notification of Miller Act Payment Bond Protection. (USCG)

____3052.228-91 Loss of or Damage to Leased Aircraft. (USCG)

____3052.228-92 Fair Market Value of Aircraft. (USCG)

____3052.228-93 Risk and Indemnities. (USCG)

____3052.236-70 Special Provisions for Work at Operating Airports.

__X__3052.242-72 Contracting Officer's Technical Representative.

____3052.247-70 F.o.B. Origin Information.

____Alternate I

____Alternate II

____3052.247-71 F.o.B. Origin Only.

__X__3052.247-72 F.o.B. Destination Only.

**(End of clause)**

**Personal Conflicts of Interest and Procurement Integrity**

In addition to the Organization Conflict of Interest Plan, the Contractor shall ensure that all personnel assigned to resulting task order(s) sign permanent non-disclosure agreements and procurement integrity certifications as required by the Contracting Officer (CO). All personnel assigned to resulting task order(s) shall immediately notify the CO in writing of any potential conflicts of interest that may be perceived through their performance on the resulting task order(s). The CO will determine if the particular individual or group of individuals will be excluded from any acquisition/project. In the event such a determination is made, the CO will provide immediate oral notification (followed by written notification within five days thereafter) of the individuals and the situation that precludes their performance under the resulting task order. The Contractor shall immediately (within five (5) days after receipt of oral notification) remove the individual(s) from the resulting task order and identify their replacement.

**(End of clause)**

**CGAP SUBCHAPTER 3004.1301-90 Contract clause**

**Trusted Associate Sponsorship System (TASS)**

(a) "Contractor employee" means an employee of a firm, or an individual, under contract or subcontract to the Coast Guard to provide services and who requires physical and/or logical access to information systems and/or facilities.

(b) Homeland Security Presidential Directive (HSPD)-12 mandates a Federal standard for secure and reliable forms of identification for Federal employees and contractor employees. The Common Access Card (CAC) is a personal identification card for the Department of Defense/Uniformed Services and complies with HSPD-12. The Coast Guard has instituted the CAC as its HSPD-12 compliant personal identification card for contractor and subcontractor employees who are required to access a Coast Guard, Department of Defense (DOD), or other federally-controlled computer information system and/or facility, or need public key infrastructure (PKI) authentication to perform their contractual duties. The Trusted Associate Sponsorship System (TASS) is the automated application process for obtaining a CAC.

(c) Contractor and subcontractor employees working pursuant to this contract who are required to access a Coast Guard, DOD, or other federally-controlled computer information system and/or facility, or need PKI authentication to perform their contractual duties shall use TASS to obtain a CAC.

(d) The Contracting Officer Representative (COR) shall serve as the TASS Trusted Agent and is responsible for creating contractor accounts in the TASS approving, returning, or rejecting CAC applications (as applicable); re-verifying assigned contractors every six months; revoking contractor and employee eligibility for a CAC; and confiscating a CAC when the contract expires or when a contractor or subcontractor employee stops working under the contract.
(e) Current standards require a favorable fingerprint check and verification of an initiated or completed investigation for all incoming Coast Guard contractor personnel before CAC issuance. The COR shall ensure that contractor personnel satisfy the security requirements for CAC issuance, and that completed fingerprint cards and electronic questionnaires for investigation processing are submitted to the U.S. Coast Guard Security Center (SECCEN).

(f) The COR or Contracting Officer shall provide such forms to, or request such information from, contractor employees that may be necessary for obtaining a CAC via the TASS. Completed forms and information shall be submitted as directed by the COR or Contracting Officer. Contractors are responsible for the accuracy and completeness of the information submitted and for any liability resulting from the Government’s reliance on inaccurate or incomplete information.

(g) Contractor or subcontractor employees who are declined via the TASS are ineligible to perform work under this contract. When an employee with a CAC is no longer performing work under this contract, the employee must return them to the COR or Contracting Officer on the same day the employee stops working.

(h) The contractor shall insert this clause in all subcontracts when a subcontractor’s employee is required to access a Coast Guard, DOD, or other federally-controlled computer information system and/or facility, or need PKI authentication to perform contractual duties.

**(End of clause)**

# RFQ 70Z0G319QPBZ02900: AUXDATA Pricing Matrix

**NOTE:** Offerors shall complete all applicable yellow fields in this sheet. The Government requires an hourly rate for all Offeror specified labor categories. For all Post Implementation Service Periods of Performance, an offeror may either provide a single service cost as an ODC or detail the service cost with any combination of labor and ODC.

| Base Period: Implementation/Transition Phase (TBD # Months) | | | | | | |
|---|---|---|---|---|---|---|
| C4ITSC Labor Category | GSA Rate | BPA Discount % | Total Discount | Total Discounted Hourly Rate | Estimated Hours | Total Price |
| | | | - | - | | - |
| | | | - | - | | - |
| | | | - | - | | - |
| | | | - | - | | - |
| | | | - | - | | - |
| | | | - | - | | - |
| | | | - | - | | - |
| | | | - | - | | - |
| | | | - | - | | - |
| | | | - | - | | - |
| | | | - | - | | - |
| | | | - | - | | - |
| | | | - | - | | - |
| | | | - | - | | - |
| | | | - | - | | - |
| | | | - | - | | - |
| | | | - | - | | - |
| Total Base Period (Labor) | | | | | - | - |
| Other Direct Costs | | | | | | - |
| Estimated Travel Costs (see Note) | | | | | | - |
| Total Base Period (Labor + Travel) | | | | | | - |

**Note:** There will be no G&A rate factored into the Estimated Travel Costs.

| Base Period: • Service Management Phase (12 months minus # of months proposed for implementation) | | | | | | |
|---|---|---|---|---|---|---|
| Total | | | | | | - |

| Option Period 1 • Service Management Phase (12 months) | | | | | | |
|---|---|---|---|---|---|---|
| Total Option Period 1 | | | | | | - |

| Option Period 2 Service Management Phase (12 months) | | | | | | |
|---|---|---|---|---|---|---|
| Total Option Period 2 | | | | | | - |

| Option Period 3 Service Management Phase (12 months) | | | | | | |
|---|---|---|---|---|---|---|
| Total Option Period 3 | | | | | | - |

| Option Period 4 Service Management Phase (12 months) | | | | | | |
|---|---|---|---|---|---|---|
| Total Option Period 4 | | | | | | - |

| Total Price (Base & Options): 60 months | - |
|---|---|

# ATTACHMENT 4 SPECIAL CONTRACT REQUIREMENTS

## H.1. Introduction

All requirements stated in the following sections will be required for all task orders issued under this contract. Specific application of Security Requirements will be provided for each TO.

## H.2. Security Requirements

All contractor personnel working under this contract, at a minimum, must have a favorable fingerprint check and have the minimum Tier 1 investigation initiated or completed in order to obtain a Department of Defense (DoD) Common Access Card (CAC).

All contractor personnel who require privileged access to systems must possess, at a minimum, a favorable Tier 1 investigation for unclassified systems.

A list of contractors working under this contract shall be provided to the Government at the time the contract is awarded on an individual Visit Access Request (VAR).

The following clauses address security clearance and access requirements:

- HSAR 3052.204-71 Contractor Employee Access Alternate I (Sep 2012)
- Safeguarding of Sensitive Information (Mar 2015)
- Information Technology Security and Privacy Training (Mar 2015)
- FAR 52.204-2 Security Requirements (Aug 1996)

Contractor employees may have access to, view, process, or otherwise come into contact with information that is sensitive, procurement sensitive, For Official use Only (FOUO), Privacy Act, or other sensitive information. These employees must sign the DHS 11000-6 Non Disclosure Agreement during orientation with OSC Command Security.

All services performed must be compliant with DHS Management Directive (MD 4300).

## H.3. Security Clearance Screening and Access

The Contractor shall furnish appropriate documentation (Joint Personnel Adjudication System (JPAS) certification will suffice or Visitor Request) to the appropriate C4ITSC unit Command Security Officer (CSO) during the initial award of the contract, and annually thereafter. Specifically, all Contractor and Subcontractor employees working under this contract who have been granted a security clearance by the Office of Personnel Management (OPM) or formerly granted by PSI-I must furnish this documentation prior to the employee commencing work. The Contractor shall inform the CSO when application materials are submitted for security investigations. The Contractor shall track and monitor progress of investigations; reporting all changes in status to the CSO, including active follow-up on all submissions.

Security screenings that reveal the following (but not limited to) may cause rejection of access to Government resources: conviction for a felony, a crime of violence or a serious misdemeanor, and/or a record of arrests for continuing offenses.

The intent and purpose of security screening and investigation are to preclude the assignment of any individual who poses a threat to the Government or to successful contract completion due to past unlawful or inappropriate behavior. The Contractor shall ensure that each prospective contract or subcontract employee furnishes all required data in the form and format determined by the Contracting Officer or the duly authorized representative.

If a Contractor employee comes under suitability investigation, (see COMDTINST M5520.12 (series) Personnel Security Program) the Contractor shall abide by the USCG Personnel Security Officer decision. This may include the removal of the employee from work performed under this Contract and/or remove access to sensitive information pending the results of an investigation.

a. The Government has the authority to grant, deny, withhold or terminate suitability determinations for Contractor employees. The Government may, as it deems appropriate, conduct background checks or grant temporary suitability determinations to Contractor employees. However, the granting of a temporary suitability determination to any Contractor employee shall not be considered as assurance that full favorable determination will follow as a result or condition thereof; and the granting of either temporary or final favorable determination shall in no way prevent, preclude or bar the withdrawal or termination of any such determination by the Government.
b. The Government for a period of up to six months may grant temporary suitability determination allowances from the date that such allowance is approved. All Contractor employees working under this Contract, after the expiration of the six month temporary determination and unless renewed one time for an additional six months, shall not work under this Contract until a full suitability determination has been completed.

## H.4. Sensitive Information

The Government has designated that all contractor employees working under this contract will require at least a Tier 1 investigation, as defined by the Department of Homeland Security. Tier 1 investigations, until otherwise determined, are based upon Contractor supplied Position Descriptions (PDs). Therefore, the company shall cooridante with the local USCG Security Office to initiate the Tier 1 investigation process. A Tier 1 request shall be submitted by the company's FSO to the local USCG Security Office using a VAR. The local USCG Security Office will intaite the SF-85 (Questionnaire for Non-Sensitive Positions) via the Office of Personnel Management's e-QIP SYSTEM. The local USCG Security Office will schedule an appointment to have the applicants fingerprints taken. The U.S. Coast Guard Security Center, CSO and Contracting Officer will use this information to determine whether or not a temporary suitability determination will be granted to allow interim access to Government resources for a particular proposed employee until a final suitability determination can be made for privilege users. Documented proof of security clearances granted by OPM can be provided in lieu of these forms.

The Contracting Officer and CSO will designate the level of screening for a given position based on an evaluation of risk, benefit/cost, and feasibility. In order to facilitate the proper assigning of security criticality levels for each Contractor employee, the Government requires position descriptions (PDs) for all labor categories proposed. The PD descriptions shall be based on the contract labor categories proposed, and be tailored to the Contractor's personnel and management structures.

Following contract award, the Contracting Officer will use these PDs to evaluate each position for sensitivity and criticality, and then assign a criticality level. The guidelines for reviewing and assigning criticality levels are stipulated in Commandant Instruction (COMDTINST) M5520.12 (series) and COMDTINST M5500.13 (series) Chapter 6.

## H.5. Access to Government Resources

By requesting access, the Contractor is certifying that all Contractor personnel involved in the management, use, and operation of systems under this Contract have received training appropriate to their assignment as defined in NIST Special Publication 500-172 Computer Security Training Guidelines.

## H.6. 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:

(i) Truncated SSN (such as last 4 digits)
(ii) Date of birth (month, day, and year)

(iii) Citizenship or immigration status
(iv) Ethnic or religious affiliation
(v) Sexual orientation
(vi) Criminal History
(vii) Medical Information
(viii) 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) DoD 8510.01 Risk Management Framework July 2017
(10) Chairman Joints Staff Instruction (CJCSI) 6510.01F June 2015
(11) Federal Information Processing Standard (FIPS) 140-2 Security Requirements for Cryptographic Modules accessible at http://csrc.nist.gov/groups/STM/cmvp/standards.html
(12) 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
(13) NIST Special Publication 800-88 Guidelines for Media Sanitization accessible at http://csrc.nist.gov/publications/PubsSPs.html
(14) Risk Management Framework (RMF) for DoD InformationTechnology (IT), DoDI 8510.01 (series)

(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 Assessment and Authorization (A&A) process as defined below.

(1) Complete the A&A process. The A&A process shall proceed according to the *DHS Sensitive Systems Policy Directive 4300A* (Version 13.1, July 27, 2017), or any successor publication, and *DHS 4300A Sensitive Systems Handbook* (Version 12, November 15, 2015).

(i) A&A Documentation. A&A documentation shall be developed using the Government provided Requirements Traceability Matrix and Government security documentation templates. A&A 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 A&A documentation, the Contractor shall submit a signed A&A 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 A&A package and may limit the number of resubmissions of a modified A&A 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 A&A 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 A&A package to the Government for acceptance.

(iii) Support the completion of the Privacy Threshold Analysis (PTA) as needed. As part of the A&A 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 A&A package as part of the ATO renewal process. The Contractor shall update its A&A package by one of the following methods: (1) Updating the A&A 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 A&A 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 *(current fiscal year)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*.

## H.7. 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.

## H.8. Revocation of Access to Government Resources

The Contractor shall maintain a list of personnel with completed clearances and security screenings. Access to Government resources shall be revoked if an individual becomes a threat to the Government resources. The Government may remove network or system access privileges from Contractor personnel for unauthorized, negligent or illegal actions.

If a Contractor employee is fired or leaves the Contract or company under adverse conditions, the Contractor shall notify the Contracting Officer, CSO, and ISSO.

## H.9. Privacy Act Notification

The personal information maintained in any system of records provided to, designed, developed or operated by the Contractor under the terms of this Contract is to be accorded the full protection of the Privacy Act of 1974. Access to information must be limited to authorized USCG personnel or employees of the Contractor working directly on this Contract who have a valid need to know.

Equipment and management controls must be adequate to prevent unauthorized access or disclosure which might result from concurrent utilization of computer resources by multiple, independent users.

No dissemination or use of these records obtained by the Contractor from the USCG shall be permitted except in accordance with the terms of this Contract and the modifications thereto. Furthermore, any records, data, reports, information, or other documentation generated for the USCG, subject to the Privacy Act, are property of the USCG and such material, as well as those records originally provided pursuant to this Contract, shall be returned to the USCG upon completion of the terms of the Contract.

It is the Contractor's responsibility under the terms of the Privacy Act for the purposes of this Contract to familiarize and brief the Contractor's employees involved with this Contract on the conditions of the Privacy Act of 1974.

## H.10. Personnel Requiring Access to Government Facilities

The Contractor shall provide an initial list of Contractor personnel who require access to the Government installation during the course of the Contract to the Contracting Officer at the post-award conference. If Contractor personnel change during the term of the Contract, the Contractor shall provide a revised list to the Contracting Officer five days prior to Contractor

personnel requiring access to the installation. (*NOTE: All key personnel changes must be in accordance with HSAR Clause 3052.215-70, Key Personnel or Facilities (DEC 2003).*

- **Qualified Personnel** - In addition to the Tier 1 minimum investigation, each employee of the Contractor shall be a citizen of the United States of America and have on file a DHS 11000-6 Non-Disclosure Agreement (NDA).
- **Employee Identification** - Visiting Contractor employees shall comply with all Government escort rules and requirements. All Contractor employees shall identify themselves as Contractors when their status if not readily apparent and display all identification and visitor badges in plain view above the waist at all times.
- **Employee Conduct** - Contractor employees shall present a professional appearance at all times and their conduct shall not reflect discredit upon the United States, the Department of Homeland Security, or the United States Coast Guard.
- **Conflict of Interest** - The Contractor shall not employ any person who is an employee of the United States Government if that employment would, or would appear to cause a conflict of interest.
- **Security** - Contractor access to information protected under the Privacy Act is required under this Contract. Contractor employees shall safeguard this information against unauthorized disclosure or dissemination in accordance with the law and Government policy and regulation.

## H.11. Non-Supervision of Contractor Employees

The Government shall not exercise any supervision or control over Contractor employees performing services under this contract. The Contractor's employees shall be accountable solely to the Contractor's management, who in turn is responsible to the Government.

## H.12. Pass Down To Subcontracts

The following requirements of the prime contract shall be included in subcontracts, awarded by the Contractor:

a. HSAR 3052.209-72 Organizational Conflicts of Interest
b. Key Personnel
c. The Contractor shall pass down to subcontractor(s) Contract requirements necessary to ensure that products, services and documentation delivered to the Government are developed in accordance with prime Contractor requirements.

## H.13. DHS CIO Compliance Clauses

### H.13.1. Section 508 Accessibility Requirements

**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**

Section 508 of the Rehabilitation Act, as amended by the Workforce Investment Act of 1998 (P.L. 105-220) (codified at 29 U.S.C. § 794d) requires that when Federal agencies develop, procure, maintain, or use information and communications technology (ICT), it shall be accessible to people with disabilities. Federal employees and members of the public with disabilities must be afforded access to and use of information and data comparable to that of Federal employees and members of the public without disabilities.

- All products, platforms and services delivered as part of this work statement that, by definition, are deemed ICT or that contain ICT shall conform to the revised regulatory implementation of Section 508 Standards, which are located at 36 C.F.R. § 1194.1 & Apps. A, C & D, and available at https://www.gpo.gov/fdsys/pkg/CFR-2017-title36-vol3/pdf/CFR-2017-title36-vol3-part1194.pdf. In the revised regulation, ICT replaced the term electronic and information technology (EIT) used in the original 508 standards.

  Item that contains Information and Communications Technology (ICT): Software Application

  Applicable Exception: N/A  Authorization #: N/A

  Applicable Functional Performance Criteria: All functional performance criteria in Chapter 3 apply to when using an alternative design or technology that results to achieve substantially equivalent or greater accessibility and usability by individuals with disabilities than would be provided by conformance to one or more of the requirements in Chapters 4 and 5 of the Revised 508 Standards, or when Chapters 4 or 5 do not address one or more functions of ICT.

  Applicable 508 requirements for electronic content features and components (including Internet and Intranet website; Electronic documents; Electronic forms; Electronic document templates; Electronic reports): All requirements in E205 apply, including all WCAG Level AA Success Criteria Apply

  Applicable 508 requirements for software features and components (including Web, desktop, server, mobile client applications; Service Offerings): All requirements in Chapter 5 apply, including all WCAG Level AA Success Criteria, 502 Interoperability with Assistive Technology, 503 Application, 504 Authoring Tools

  Applicable 508 requirements for hardware features and components: Does not apply

Applicable 508 requirements for support services and documentation: All requirements in Chapter 6 apply

- When providing and managing hosting services for ICT, the contractor shall ensure the hosting service does not reduce the item's original level of Section 508 conformance before providing the hosting service.
- When providing installation, configuration or integration services for ICT, the contractor shall not reduce the original ICT item's level of Section 508 conformance prior to the services being performed.
- When providing maintenance upgrades, substitutions, and replacements to ICT, the contractor shall not reduce the original ICT's level of Section 508 conformance prior to upgrade, substitution or replacement. The agency reserves the right to request an Accessibility Conformance Report (ACR) for proposed substitutions and replacements prior to acceptance. The ACR should be created using the on the Voluntary Product Accessibility Template Version 2.2 508 (or later). The template can be located at https://www.itic.org/policy/accessibility/vpat
- When developing or modifying ICT for the government, the contractor shall ensure the ICT fully conforms to the applicable Section 508 Standards. When modifying a commercially available or government-owned ICT, the contractor shall not reduce the original ICT Item's level of Section 508 conformance.
- When developing or modifying web and software ICT, the contractor shall demonstrate Section 508 conformance by providing Section 508 test results based on the versions of the DHS Trusted Tester Methodology currently approved for use, as defined at https://www.dhs.gov/compliance-test-processes. The contractor shall use testers who are certified by DHS on how to use the DHS Trusted Tester Methodology (e.g. "DHS Certified Trusted Testers") to conduct accessibility testing. Information on how testers can become certified is located at https://www.dhs.gov/publication/trusted-tester-resources.
- When developing or modifying ICT that are delivered in an electronic Microsoft Office or Adobe PDF format, the contractor shall demonstrate conformance by providing Section 508 test results based on the Accessible Electronic Documents – Community of Practice (AED COP) Harmonized Testing Guidance at https://www.dhs.gov/compliance-test-processes.
- When developing or modifying software that generates electronic content (e.g., an authoring tool that is used to create html pages, reports, surveys, charts, dashboards, etc.), the contractor shall ensure software can be used to create electronic content that conforms to the Section 508 standards.
- Contractor personnel shall possess the knowledge, skills and abilities necessary to address the applicable revised Section 508 Standards for each ICT.
- 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 Contracting Officer and a determination will be made according to DHS Directive 139-05, Office of Accessible Systems and Technology, dated January 29, 2016

and DHS Instruction 139-05-001, Managing the Accessible Systems and Technology Program, dated January 11, 2017.

- Where ICT conforming to one or more requirements in the Revised 508 Standards is not commercially available, the agency shall procure the ICT that best meets the Revised 508 Standards consistent with the agency's business needs, in accordance with 36 CFR E202.7. 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) according to DHS Directive 139-05, Office of Accessible Systems and Technology, dated January 29, 2016 and DHS Instruction 139-05-001, Managing the Accessible Systems and Technology Program, dated January 11, 2017 and 36 CFR E202.6.

## H.14. Coast Guard Information Technology Security Requirements

No Contractor personnel shall commence any performance under this Contract, requiring system access, until they:

a. Have completed the Automated Information Security (AIS) User Acknowledgement Form (CG-5500A).
b. Completed the Information Systems Security (ISS) training (COMDTINST M5500.13 (series)) from the appropriate Coast Guard Information Systems Security Officer (ISSO).
c. "Continue to complete the Information Systems Security (ISS) training annually". A copy of this user security agreement is provided as *Appendix 3 of Attachment 1* of this Contract. By signing the aforementioned user security agreement, the individual will be acknowledging their responsibility to properly use and safeguard all Coast Guard information technology resources and information related thereto. The COR for this Contract shall arrange the aforementioned security briefing.

The Contractor shall access only those areas of Coast Guard information technology resources (e.g., computer equipment, networking equipment, telecommunications equipment, cabling, network drives, computer drives, network software, computer software, software programs, intranet sites, internet sites. etc.) explicitly stated in this Contract and/or as approved by the COR 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 explicitly authorized by the Performance Work Statement, other terms and conditions in this Contract, or approved in writing by the COR is strictly prohibited. In the event of violation of this provision, the Coast Guard will take appropriate action with regard to the Contract.

Contractor access to Coast Guard computer systems and/or networks from a remote location is a temporary privilege for the mutual convenience it offers while the Contractor performs business for the Coast Guard. It is not a right, a guarantee, a condition of the Contract, nor is it Government Furnished Equipment (GFE).

Contractor access may be terminated for unauthorized use. The Contractor agrees to hold the Coast Guard harmless and the Contractor will not request additional time or money under the Contract for any delays resulting from unauthorized use.

*All hardware, software, and services provided under this contract must be compliant with DHS 4300A DHS Sensitive System Policy and the DHS 4300A Sensitive Systems Handbook.*

## H.15. Encryption Compliance:

If encryption is required, the following methods are acceptable for encrypting sensitive information:

1. FIPS 197 (Advanced Encryption Standard (AES)) 256 algorithm and cryptographic modules that have been validated under FIPS 140-2.
2. National Security Agency (NSA) Type 2 or Type 1 encryption.
3. Public Key Infrastructure (PKI) (see paragraph 5.5.2.1 of the Department of Homeland Security (DHS) IT Security Program Handbook (DHS Management Directive (MD) 4300A) for Sensitive Systems).

## H.16. Access to Unclassified Facilities, Information Technology Resources, and Sensitive Information

The assurance of the security of unclassified facilities, Information Technology (IT) resources, and sensitive information during the acquisition process and contract performance are essential to the DHS mission. DHS Management Directive (MD) 11042.1 Safeguarding Sensitive But Unclassified (For Official Use Only) Information, describes how contractors must handle sensitive but unclassified information. DHS MD 4300.1 Information Technology Systems Security and the DHS Sensitive Systems Handbook prescribe policies and procedures on security for IT resources. Contractors shall comply with these policies and procedures, any replacement publications, or any other current or future DHS policies and procedures covering contractors specifically for all contracts that require access to DHS facilities, IT resources or sensitive information. Contractors shall not use or redistribute any DHS information processed, stored, or transmitted by the contractor except as specified in the contract.

## H.17. Security Review

The Government may elect to conduct periodic reviews to ensure that the security requirements contained in this contract are being implemented and enforced. The Contractor shall afford DHS including the organization of the DHS Office of the Chief Information Officer, the Office of the Inspector General, authorized Contracting Officer's Representative (COR), and other government oversight organizations, access to the Contractor's facilities, installations, operations, documentation, databases, and personnel used in the performance of this contract. The Contractor will contact the DHS Chief Information Security Officer to coordinate and participate in the review and inspection activity of government oversight organizations external to the DHS. Access shall be provided to the extent necessary 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 DHS data or the function of computer systems operated on behalf of DHS, and to preserve evidence of computer crime.

## H.18. Interconnection Security Agreement (ISA) Requirements

Interconnections between DHS and non-DHS IT systems shall be established only through controlled interfaces and via approved service providers. The controlled interfaces shall be accredited at the highest security level of information on the network. Connections with other Federal agencies shall be documented based on interagency agreements; memoranda of understanding, service level agreements or interconnect service agreements.

## H.19. DHS Enterprise Architecture Compliance Requirements

Existing systems are considered as being aligned to the DHS Enterprise Architecture via the "Amnesty Day" list of products and standards in use at USCG prior to 31 December 2007. Any new systems that use products not contained in the DHS Technical Reference Manual (TRM) must obtain a "technical insertion" granted by DHS.

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

- All developed solutions and requirements shall be compliant with Coast Guard and Homeland Security EA.
- All IT hardware or software shall be compliant with the HLS EA Technical Reference Model (TRM) Standards and Products Profile, and with the USCG IT products and standards inventory.
- All data assets, information exchanges and data standards, whether adopted or developed, shall be submitted to the DHS Enterprise Data Management Office (EDMO) for review and insertion into the DHS Data Reference Model.
- In compliance with Office of Management and Budget (OMB) mandates, all network hardware shall be IPv6 compatible without modification, upgrade, or replacement.
- All Information Technology assets being developed, procured, or acquired shall be IPv6 capable.

## H.20. DHS Geospatial Information System Compliance Requirements

The following requirements are for incorporation into acquisition documents only when geospatial equipment or data is involved with the acquisition:

All implementations shall comply with the policies and requirements set forth in the DHS Geospatial Information Infrastructure (GII), including the following:

- All developed solutions and requirements shall be compliant with the HLS EA.

- All IT hardware or software shall be compliant with the HLS EA Technical Reference Model (TRM) Standards and Products Profile.
- All implementations shall comply with the policies and requirements set forth in the DHS Geospatial Information Infrastructure (GII).
- The DHS geospatial data model shall be used building to the GII.
- All data within the GII, whether adopted or developed, shall be submitted to the DHS Enterprise Data Management Office (EDMO) for review and insertion into the DHS Data Reference Model and Enterprise Architecture Information Repository.

## H.21. HSAR 3004.470-2

DHS policies and procedures on contractor personnel security requirements are set forth in various management directives (MDs). MD 4300.1, entitled Information Technology Systems Security, and the DHS Sensitive Systems Handbook, prescribe the policies and procedures on security for Information Technology resources. MD 11042.1, Safeguarding Sensitive But Unclassified (For Official Use only) Information describes how contractors must handle sensitive but unclassified information. Compliance with these policies and procedures, any replacement publications, or any other current or future DHS policies and procedures, covering contractors specifically, is required in all contracts that require access to facilities, IT resources or sensitive information. (b) The contractor must not use or redistribute any DHS information processed, stored, or transmitted by the contractor except as specified in the contract".

## H.22. General Requirements

The Contractor shall ensure all general requirements are expressly incorporated into any and all subcontracts or subordinate agreements issued in support of this contract.

### H.22.1. Contractor Personnel Suitability Determination

DHS may, as it deems appropriate, authorize and grant a favorable entry on duty (EOD) decision based on preliminary suitability 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. A favorable EOD decision or a full employment suitability determination shall in no way prevent, preclude, or bar DHS from withdrawing or terminating access government facilities or information, at any time during the term of the contract. No employee of the Contractor shall be allowed to work under this contract without a favorable EOD decision or suitability determination by the Security Office.

Contract employees waiting for an EOD decision may begin work on the contract provided they do not access sensitive Government information. Limited access to Government buildings is allowable prior to the EOD decision if the Contractor is escorted by a Government employee. This limited access is to allow Contractors to attend briefings, non-recurring meetings and begin transition work.

## H.22.2. Background Investigations

To comply with the requirements HSAR Clause 3052.204-71, and Department policy contractor employees (to include applicants, temporaries, part-time and replacement employees) under the Contract, requiring access to sensitive information shall undergo a position sensitivity analysis based on the duties each individual will perform on the contract. The results of the position sensitivity analysis shall identify the appropriate background investigation to be conducted. All public trust background investigations will be processed through the local USCG Security Office. The company FSO shall submit a VAR requesting a Tier 1 background investigation for the prospective contractor. Prospective Contractor employees that do not have a security clearance shall submit the following completed forms to the local USCG Security Office through their FSO unless otherwise noted:

a. Standard Form 85, "Questionnaire for Non-Sensitive Positions"
b. Optional Form 306, "Declaration for Federal Employment"
c. DHS Form 11000-9, "Disclosure and Authorization Pertaining to Consumer Reports Pursuant to the Fair Credit Reporting Act"

The Standard Form 85 will be completed electronically, through the Office of Personnel Management's e-QIP SYSTEM. The completed forms must be given to the local USCG Security Office and adjudicated by the USCG Security Center prior to entry on duty of any employees, whether a replacement, addition, subcontractor employee, or vendor.

Only complete packages will be accepted by the local USCG Security Office. Specific instructions on submission of packages will be provided upon award of the contract.

Be advised that unless an applicant requiring access to sensitive information has resided in the Unite States for three of the past five years, the Government may not be able to complete a satisfactory background investigation.

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:

a. The individual must be a legal permanent resident of the U. S. or a citizen of Ireland, Israel, the Republic of the Philippines, or any nation on the Allied Nations List maintained by the Department of State;
b. There must be a compelling reason for using this individual as opposed to a U. S. citizen; and
c. The waiver must be in the best interest of the Government.

### H.22.3. Continued Eligibility

The Contracting Officer may require the contractor to prohibit individuals from working on contracts 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.

### H.22.4. Determinations

The local USCG Security Office shall be notified of all terminations/resignations immediately. The Contractor shall return to the Contracting Officer Representative (COR) all DHS issued identification cards and building passes that have either expired or have been collected from terminated employees. If an identification card or building pass is not available to be returned, a report shall be submitted to the COR, referencing the pass or card number, name of individual to who it was issued and the last known location and disposition of the pass or card.

### H.22.5. Information Technology Security Clearance

When sensitive government information is processed on Department telecommunications and automated information systems, the Contractor shall provide for the administrative control of sensitive data being processed. Contractor personnel must have favorably adjudicated background investigations commensurate with the defined sensitivity level.

Contractors who fail to comply with Department security policy are subject to having their access to Department IT systems and facilities terminated, whether or not the failure results in criminal prosecution. Any person who improperly discloses sensitive information is subject to criminal and civil penalties and sanctions under a variety of laws (*e.g.*, Privacy Act).

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.

### H.23. Observance of Legal Holidays and Excused Absence

a. The Government hereby provides notification that Government personnel observe the listed days as holidays:

| | |
|---|---|
| (1) New Year's Day | (6) Labor Day |
| (2) Martin Luther King's Birthday | (7) Columbus Day |
| (3) President’s Day | (8) Veterans' Day |
| (4) Memorial Day | (9) Thanksgiving Day |
| (5) Independence Day | (10) Christmas Day |

b. In addition to the days designated as holidays, the Government observes the following days:

1. Any other day designated by Federal Statute
2. Any other day designated by Executive Order
3. Any other day designated by the President’s Proclamation

c. It is understood and agreed between the Government and the Contractor that observance of such days by Government personnel shall not otherwise be a reason for an additional period of performance, or entitlement of compensation except as set forth within the contract. In the event the Contractor's personnel work during the holiday, they may be reimbursed by the Contractor, however, no form of holiday or other premium compensation will be reimbursed by the Government either as a direct or indirect cost, other than their normal compensation for the time worked. Contractor personnel under this contract are considered to be professional employees, therefore there will be no reimbursement for overtime work.
d. If Federal Government personnel are furloughed, the Contractor shall continue to provide services previously funded under the task order contract. The pricing of the task order will not be affected by a Federal Government furlough.
e. Nothing in this clause abrogates the rights and responsibilities of the parties relating to stop work provisions as cited in other sections of this contract.

## H.24. Non-Personal Services

The Government and the Contractor understand and agree that the services delivered by the Contractor to the Government are non-personal services. The parties also recognize and agree that no employer-employee or master-servant relationship exists or will exist between the Government and the Contractor's employees. The Contractor and the Contractor's employees are not employees of the Federal Government and are not eligible for entitlement and benefits given Federal employees.

Contractor personnel under this contract shall not (i) be placed in a position where there is an appearance that they are employees of the Federal Government, or are under the supervision, direction, or control of or are evaluated by a Federal Official, or (ii) be placed in a position of command, supervision, administration, or control over Government personnel.

## H.25. Identification of Contractor Personnel

The Contractor shall ensure that its employees will identify themselves as employees of their respective company while working on DHS/USCG contracts. For example, contractor personnel shall introduce themselves in person and in voice-mail, as employees of their respective companies, and not as DHS/USCG employees. The Contractor shall ensure that their personnel use the following format signature on all official e-mails generated by DHS/USCG computers:

- Name
- Position or Professional Title
- Company Name
- USCG *Unit Name*
- Phone
- Fax
- Other contact information as desired

## H.26. Department of Defense (DoD) Directive 8570 Contractor Compliance

All contractor personnel shall be required to maintain a professional certification in accordance with the Department of Defense 8570.01-M, *Information Assurance Workforce Improvement Program.* As a condition of privileged access to any information system, personnel performing IA functions as described in the Information Assurance Workforce Improvement Program, DoD 8570.01-M, shall satisfy and sustain DoD IA training and certification requirements (see DoD 8570.01-M, Chapters 3, 4, 6, and 11). IAT Computing Environment certifications are not required.

Contractor employee classifications are as follows:

- SME Level I (Junior/Apprentice)
  Minimum requirement is IAT-II or IAM-I for privileged access.

- SME Level II (Mid/Journeyman)
  Minimum requirement is IAT-II or IAM-I for privileged access.

- SME Level III (Senior)
  Minimum requirement is IAT-III or IAM-II for privileged access

Upon request by the Government, the Contractor shall provide documentation supporting the Department of Defense 8570.01-M certification status. Contractor personnel who do not have proper and current certifications shall be denied access to DOD information systems. All Contractor employees shall be citizens of the United States, and meet the security background criteria as defined in Section H. All Contractors, to include internal and external consultants and/or support staff must also meet required security criteria. All Contractor personnel must have a favorably adjudicated background investigation as defined by the USCG prior to being granted access to a USCG IT System. The Contractor will be held responsible for applying for, obtaining and maintaining a valid Common Access Card (CAC) as a condition of continued employment under the contract.

## H.27. Department of Defense Cybersecurity Activities Performed for Cloud Service Offerings

The contractor shall ensure compliance with DoD memorandum "Department of Defense Cybersecurity Activities Performed for Cloud Service Offerings" and understand the boundary between the functions performed by the Government and functions performed by the Cloud Service Provider (CSP). Per the memo the following cybersecurity activities will be performed by either the Government or the Contractor indicated by the X:

| Cyber Security Activity | Government | Contractor |
|---|---|---|
| **External Assesment*** | | |
| DoD Cyber Red Team Operations | **X** | |
| Non-DoD Red Team | | **X** |
| Penetration Testing | | **X** |
| Intrustion Assessment | | **X** |

| | | |
|---|---|---|
| **Vulnerability Management** | | |
| Apply DoD required security configurations | | **X** |
| Perform actions to mitigate potential vulnerabilities or threats | | **X** |
| Monitor vulnerability management compliance | | **X** |
| Report Vulnerability Management Compliance | **X** | |
| **Malware Protection** | | |
| Malware protection implementation | | **X** |
| Malware Notification | **X** | |
| **Information Security Continuous Monitoring (ISCM)** | | |
| Maintain continuous visibility into endpoint devices | | **X** |
| Correlate asset and vulnerability data with threat data | **X** | |
| **Cyber Incident Handling** | | |
| Network Security Monitoring/Intrusion Detection for Boundary Cyberspace Protection functions | **X** | |
| Networkand endpoint security monitoring at the enclave level | | **X** |
| Incident reporting | **X** | |
| Incident response- Analysis | | **X** |
| Incident Handling Response | | **X** |
| **DODIN User Activity Monitoring (UAM) for DoD Insider Threat Program** | | |
| Employ UAM capabilities to detect anomalous insider activity | | **X** |
| Maintain insider threat audit data | | **X** |
| Correlate insider threat audit data with Counter Intilligence | **X** | |
| **Warning Intelligence and Attack Sensing and Warning (AS&W)** | | |
| AS&W for BCP | **X** | |
| AS&W at the Application | | **X** |
| Warning Intelligence | **X** | |
| **Information Operations Condition (INFOCON) & Orders Compliance/Network Operations (NETOPS) Awareness** | | |
| INFOCON & Orders Implementation | | **X** |
| INFOCON & Orders Notification and Assistance | **X** | |
| **Mission Ownder Support and Cyber Security Training** | | **X** |

*** An external assessment must be performed annually. The AO will select the external assessment(s) that best fit the need of the application or mission system. The AO has the option to choose all of the external assessments, but only one is required annually.**

The contractor will be expected to perform all cybersecurity activities and provide the necessary data to enable the Government to perform its cybersecurity functions, outlined in the table above.

# ATTACHMENT 5 – RFQ INSTRUCTIONS AND EVALUATION FOR AWARD

## Introduction:

### 1.1. Offeror Questions/Clarifications

All Offeror questions and clarifications pursuant to this RFQ must be received by the Contracting Officer, Brenda.E.Oberholzer@uscg.mil, and Contract Specialist Kristi Durbin no later than **April 26 2019 at 3:00 PM, EDT**. The Government reserves the right not to provide a response for any Offeror question/clarification received after the date and time stated above. If, however, the Contracting Officer determines that a request cites an issue of significant importance, the Government will provide a written response to all Offerors.

The Government will not provide information in response to telephone calls. Contacting other USCG personnel regarding this solicitation in an attempt to gain procurement-sensitive information may result in disqualification from the evaluation process. Written responses to all Offeror questions/clarifications will be sent to GSA IT Schedule 70 contract holders NAICS 518210, SIN 132-51 "Information Technology Professional Services" Offerors with due regard to the proper protection of proprietary information via an amendment to the solicitation.

### 1.2. Ordering Period

The BPA ordering period includes a 12 month base period and four 12 month option periods for a total of 60 months beginning date of award.

### 1.3. Specific Requirements

See the BPA Statement of Work (Attachment 1). For evaluation purposes, and with the intent to award as a call, the AUXDATA Modernization Statement of Work (Attachment 6) is also provided.

### 1.4. Quotation Preparation and Delivery Instructions

The Phase I submission shall consist of: (1) Signed cover letter certifying that the Offeror has read and agrees to comply with all of the conditions and instructions provided in this RFQ document, and all amendments issued; (2) Prior experience submission.

Phase II will not require anything additional to be submitted but instructions and coordination will be communicated via email.

Phase III submission shall consist of: (1) Signed cover letter certifying that the Offeror has read and agrees to comply with all of the conditions and instructions provided in this RFQ document, and all amendments issued; (2) Schedule and (3) Price Matrix.

Signed cover letters must provide the following information:

A. Name of Offeror
B. Address

C. City, State, Zip code
D. Data Universal Numbering System (DUNS) Number & CAGE Code
E. Taxpayer Identification Number (TIN)
F. Points of Contact (Primary & Alternate) for both Technical and Pricing Submissions
G. Telephone Number
H. Electronic Mail Address
I. Solicitation/Quotation number
J. Date of Quotation
K. GSA Schedule Contract Number
L. Small Business Representations made by the Offeror
M. Prompt Payment Terms
N. A statement specifying the extent of agreement with all terms, conditions, and provisions included in the solicitation without exceptions or assumptions.
O. Names and contact information of persons authorized to negotiate on the Offeror's behalf with the Government in connection with this solicitation.
P. Name, title, and signature of person authorized to sign the quotation.
Q. Current Performance Period the GSA Schedule with Option Periods as applicable
R. A Statement certifying that the proposed solution falls within the scope of the Offeror's referenced GSA Schedule contract(s) as applicable by signing the cover letter.

All submissions MUST cite the applicable GSA Schedule contract number in all documents submitted in response to this RFQ.

### 1.4.1. Quotation Submission

Please review the requirement and respond via email to the Contracting Officer with a courtesy intent to provide a quote or no-quote decision as soon as possible.

**Electronic Submissions:** The Offeror shall provide an electronic copy of its Phase I quote submission via GSA's eBuy. Submission must occur prior to the Quotation Submission Deadline specified in Section 1.4.3 of this attachment.

### 1.4.2. Quotation Preparation

The Government will not consider pages submitted in excess of the stated page limitations, or materials not included in full text within the quote (no links to external information will be reviewed or considered. Page limitations include all text, graphs, pictures, appendices, references, exhibits, etc. Tabs, index sheets, tables of contents, dividers and other such aids that are solely used to assist the evaluator in locating information and are advisory in nature, imparting no other information other than the identification of content, will not be counted against any page limits stated within this RFQ.

| Phase | Volume | Not to Exceed Page Limits |
|---|---|---|
| Phase I | Factor 1: Prior Experience | 10 pages |
| Advisory Notice | | |

| | | |
|---|---|---|
| Phase II | Factor 2: Technical Solution | Technical Demonstration |
| | Factor 3: Technical Approach | Oral Presentation |
| Advisory Notice | | |
| Phase III | Factor 4: Schedule | 3 Pages |
| | Factor 5: Price | Attachment #3 Price Matrix; Representations & Certifications as required by 52.212-3 and copy of Offeror's GSA Schedule Contract shall be included in the price matrix submission. |

All narrative text contained in the quote response must be formatted to 8 ½ x 11 paper with margins of at least 1" at the top, bottom, and both sides; using single spaced, Times New Roman 12 point font. For charts, tables, exhibits and figures, no less than 8 point Times new Roman font is acceptable. Offerors are cautioned that quotation elements using a font less than 12-point Times New Roman for the narrative and less than 8-point Times New Roman for charts will not be reviewed by the Government.

### 1.4.3. Quotation Submission Deadline

Offerors shall submit Phase I: Prior Experience responses no later than **3:00 pm, EDT May 17, 2019.**

Submission deadlines for the later Phases will be detailed in future instructions provided by the Government. Following Government advisory recommendation post Phase I, Offerors will have approximately 2 business days to notify Government of interest to proceed to Phase II; actual timeline will be communicated within the notification. The Offeror will have at least 2 weeks from the Government's receipt of the Offeror's decision to proceed to prepare the submission for Phase II. Following Government advisory recommendation post Phase II, Offerors will have approximately 2 business days to notify the Government of interest to proceed to Phase III; actual timeline will be communicated within the notification. Each Offeror will have at least 2 weeks to prepare and submit Phase III upon receipt of instructions for Phase III.

Failure to participate in Phase I of the solicitation precludes further consideration of an Offeror. Submissions will not be accepted from Offerors who have not submitted the Phase I quote by the due date and time stated in this RFQ. Additionally, an Offeror's decision not to participate in Phase II of the procurement precludes further consideration of an Offeror. Finally, the Offeror's decision not to participate in Phase III of the procurement precludes further consideration of an Offeror and renders them ineligible for award.

### 1.5. Breakdown of Evaluation Factors

| Technical Factors | Business Factors |
|---|---|
| 1. Prior Experience | 4. Schedule |
| 2. Technical Solution | 5. Price |
| 3. Technical Approach | |

### 1.6. Specific Submission Instructions Relative to the Submission Phase

Offerors are advised that if they are unable to meet all requirements in Attachment 6 then they will not be eligible for award. Offerors are encouraged to articulate how the proposed tool will allow for future Workforce Management capabilities above and beyond the initial task order specified in Attachment 6 under future task orders through the BPA. Offerors are cautioned that the quality of their quotation and adherence to RFQ response requirements and/or restrictions, are considered reflective of the manner in which Offerors will be expected to perform work under this BPA. This will be given due consideration throughout the evaluation process. Offerors are strongly encouraged to emphasize content in response to all RFQ requirements.

The Government will be conducting the evaluation in three phases. **Evaluations will be based on the requirements specified in Attachment 6 AUXDATA Modernization Statement of Work.**

**Phase I**: The Government will be evaluating **Factor 1: Prior Experience**. The Offeror shall provide a maximum of three (3) examples of experience, of its own experience (the prime not the experience of any proposed subcontractors or their teaming partners). The examples of prior experience must be for contracts that are ongoing or completed within the past three (3) years from the date of the solicitation. Offerors shall furnish examples of experience that collectively demonstrate results in all of the following areas:

- Implementing a cloud-hosted application for a Federal Government/DoD entity at FedRAMP Moderate Baseline or higher (DODIN experience is preferred).
- Managing the cloud-hosted application being proposed for a Federal Government/DoD entity at FedRAMP Moderate Baseline or higher (DODIN experience preferred). This should include details on:
    - Number of users of the application
    - Handling and implementing change requests
    - Patching and completing security updates. Were there any breaches? If there were what was the cause? Were there ever any functional/usability issues caused by a new patch and how were they corrected?
    - Meeting service level agreements. Offeror should include what service levels (such as availability) they were required to meet and if they ever were unable to meet them.
    - Handling and correcting trouble tickets, incidents, and problems. Include the volume of tickets handled.
- Transitioning data and services to a cloud-hosted Software-as-a-Service for a Federal Government/DoD entity at FedRAMP Moderate Baseline or higher (DODIN experience is preferred). The Offeror should include the type and size of the data transferred, number of users, and explain how the overall strategy of transition was conducted.
- Meeting and maintaining cybersecurity authorizations and accreditations at FedRAMP Moderate baseline or higher (DODIN experience is preferred).

The Offeror must respond to the following in each submission as they pertain to the topic areas listed above:

(1) Explain how the submission meets one or more of the criteria.
(2) Describe problems, failures, or data breaches that occurred during performance of the example and what actions were taken to overcome them and ensure quality of performance.
(3) Describe difficulties or constraints that occurred and what the company did to overcome them.
(4) Describe challenges related to keeping software compliant with evolving cyber security requirements?

The Government is more interested in the quality and similarity of the experience examples to the requirement than the quantity of examples. The Offeror shall include the following information for each example:

(1) The name and contact information of a reference that can substantiate the experience and results.
(2) Contract Number. Only one contract per example;
(3) Agency that contract was performed for;
(4) Contract Period of Performance (effective date and expiration date)'
(5) Contract value;
(6) Contract Type.

Any example that does not comply with the above instructions will not be evaluated.

The information shall be sufficiently detailed that the Government can determine whether the example(s) demonstrate the prime contractor's experience. The Government will not contact the reference to obtain detail lacking from the Offeror's response.

After the Government completes evaluation of the Phase I submission, Offerors will receive an advisory notification via email from the KO. The notification will advise the Offeror of the Government's advisory recommendation to proceed or not to proceed to Phase II. Offerors who are rated most highly will be advised to proceed to Phase II of the proposal submission process. Offerors who were not among the most highly rated will be advised that they are unlikely to be viable competitors, along with the general basis for the Government's advisory recommendation. The intent of this advisory notice is to minimize development and other costs for those offerors with little to no chance of receiving an award. The Government's advice will be a recommendation only and those Offerors who are advised not to proceed may elect to continue their participation in the procurement.

The Government does not intend to provide debriefings after the completion of the advisory notifications.

**Phase II:** The Government will be scheduling Technical Demonstrations/Oral Presentations to evaluate Factor 2: Technical Solution and Factor 3: Technical Approach. The Offeror shall prepare and provide an in person demonstration with the Government where they will be exhibit their proposed solution's capability in performing selected requirements and an oral presentation discussing their technical approach. The list of requirements and capabilities the Offeror will be expected to demonstrate will be sent out with the specific instructions for Phase II. Any parts of the technical solution and oral presentation, including but not limited to responses to questions,

may be incorporated in the AUXDATA call.

Specific timelines and instructions for the demonstration, including sample data, will be provided by the Government at least 2 weeks prior to the Offeror's scheduled demonstration/oral presentation.

After the Government completes evaluation of the Technical Demonstrations/Oral Presentations, Offerors will receive an advisory notification via email from the KO. The notification will advise the Offeror of the Government's advisory recommendation to proceed or not to proceed to Phase III. Offerors who are rated most highly will be advised to proceed to Phase III of the proposal submission process. Offerors who were not among the most highly rated will be advised that they are unlikely to be viable competitors, along with the general basis for the Government's advisory recommendation. The intent of this advisory notice is to minimize development and other costs for those offerors with little to no chance of receiving an award.
The Government's advice will be a recommendation only, and those offerors who are advised not to proceed may elect to continue their participation in the procurement.

The Government does not intend to provide debriefings after the completion of the advisory notifications.

**Phase III:** The final phase will require submission of Factor 4: Schedule and Factor 5: Price. This phase requires a written response. The Schedule may be incorporated in the AUXDATA call. The Price submissions may be incorporated in the BPA and AUXDTA call as applicable. Specific instructions including limitations and deadlines will be provided to those Offerors that elect to proceed to this phase at least 2 weeks prior to the submission due date.

### 1.7. Evaluations and Selection

Evaluations will be conducted in accordance with FAR Part 8.4. The BPA will be established with the Offeror whose quotation for the AUXDATA Modernization Statement of Work (Attachment 6) represents the best value to the Government. For the purposes of this RFQ, "best value" is defined as the procurement process resulting in the most advantageous acquisition decision for the Government and is performed through an integrated assessment and trade-off analysis among the five evaluation factors. The Government may elect to award to other than the lowest priced quote, based on the results of the tradeoff analysis between non-price and price factors. The Government intends to evaluate quotations and award a single-award BPA without communications with Offerors. The Offerors should therefore propose their best approach to meeting the requirements of the SOW and solicitation. However, the Government reserves the right to enter into communications if it is deemed to be in the best interests of the Government.

Quotations submitted in response to the RFQ will be evaluated based on the following evaluation Factors:

Factor 1: Prior Experience
Factor 2: Technical Solution
Factor 3: Technical Approach
Factor 4: Schedule

Factor 5: Price

All technical factors are weighted in order of importance, with Factor 1 (Prior Experience) being more important than Factor 2 (Technical Solution), and both Factors 1 and 2 being more important than Factor 3 (Technical Approach). Of the business factors, Factor 4 (Schedule) is more important than Factor 5 (Price). When combined, Factors 1, 2, and 3 are more important than Factors 4 and 5.

The Government will be conducting the evaluation in three phases. Phase I will evaluate Prior Experience. An offeror must submit a quote for Phase I to be considered for award; failure to submit a quote in Phase I precludes an Offeror from submitting a quote for Phase II and III. Phase II will evaluate the Technical Solution and Technical Approach presented in the Technical Demonstration and Oral Presentation by the Offerors who are selected or who elect to participate in Phase II. Phase III will evaluate Factors 4 and 5 for the Offerors who are selected or who elect to participate in Phase III. Notifications will be sent out between Phase I and II and Phase II and III.

Once the government determines that an Offeror is the best-suited (e.g. the apparent successful awardee), the government reserves the right to engage with only that firm to address any remaining issues, if necessary, and finalize a task order with that firm. If the parties cannot successfully address any remaining issues, as determined pertinent at the sole discretion of the government, the government reserves the right to engage the next best-suited firm based on the original analysis and address any remaining issues. Once the government has engaged the next best-suited firm, no further engagements with the previous firm will be entertained until after the task order has been awarded. This process will continue until an agreement is successfully reached and a task order is awarded.

### 1.7.1. Phase I – Factor 1

The Government will evaluate the prime Offeror's prior experience for its confidence in the Offerors ability to successfully perform the task order requirements based on its Prior Experience of contracts that are ongoing or completed within 3 years of the date of the solicitation related to all of the following areas:

- Implementing a cloud-hosted application for a Federal Government/DoD entity at FedRAMP Moderate Baseline or higher (DODIN experience is preferred).
- Managing a cloud-hosted application for a Federal Government/DoD entity at FedRAMP Moderate Baseline or higher (DODIN experience is preferred). This should include details on:
    - Number of users of the application
    - Handling and implementing change requests
    - Patching and completing security updates. Were there any breaches? If there were what was the cause? Were there ever any functional/usability issues caused by a new patch and how were they corrected?
    - Meeting service level agreements. Offeror should include what service levels (such as availability) they were required to meet and if they ever were unable to meet them.

    - Handling and correcting trouble tickets, incidents, and problems. Include the volume of tickets handled.
- Transitioning data and services to a cloud-hosted Software-as-a-Service for a Federal Government/DoD entity at FedRAMP Moderate Baseline or higher (DODIN experience is preferred). The Offeror should include the type and size of the data transferred, number of users, and explain how the overall strategy of transition was conducted.
- Meeting and maintaining cybersecurity authorizations and accreditations at FedRAMP Moderate baseline or higher (DODIN experience is preferred).

Responses to the questions/requested information as set forth in Paragraph 1.6, Phase I, Factor 1, above will contribute to the assessment and the rating given for this factor. Ratings will be made in terms of the Government's confidence in the Offeror's prior experience and ability to meet the requirements. The Government is more interested in the quality and similarity of the Prior Experience examples to the requirement than the quantity of examples.

### 1.7.2. Phase II – Factors 2 & 3

#### 1.7.2.1 Factor 2: Technical Solution

The Government will assess each Offeror's demonstration for its confidence in the proposed technical solution and its ability to meet the mission needs of the Auxiliarists based on the technical demonstration and responses to questions. This includes the following characteristics:

**Fitness:** Does the technology address the problem at hand, or is it being used for an unintended purpose?

**Simplicity**: Is the design of the solution easily understood?

**Usability:** Is the solution intuitive and easy to use? Will individuals with little technical understanding be able to use it with minimum guidance?

**Adaptability:** How easily can the solution modified to meet new requirements or requirements of similar workforce management systems.

#### 1.7.2.2 Factor 3: Technical Approach

The Government will evaluate its overall confidence in the Offeror's Technical approach based on the oral presentation and answers to questions.

### 1.7.3. Phase III – Factors 4 & 5

#### 1.7.3.1. Factor 4: Schedule

The Government will evaluate each Offeror's schedule with respect to how quickly they can implement a solution, and transition the current AUXDATA to the new solution. The Government has set a target date for this to be complete by 6 months after contract award.

Schedule significance will increase as the Prior Experience, Technical Demonstration and Technical Approach equivalence, possibly promoting Schedule to a determinative factor.

### 1.7.3.2. Factor 5: Price

The Government will evaluate each Offeror's total evaluated price with respect to reasonableness based on the total evaluated price as stipulated in the Government's Price Matrix (Attachment 3). The total evaluated price consists of the total evaluated price for the base period and the four option periods.

Price significance will increase as the Prior Experience, Technical Demonstration and Technical Approach equivalence, possibly promoting price to a determinative factor.

**Selection for Award**
All technical factors are weighted in order of importance, with Factor 1 (Prior Experience) being more important than Factor 2 (Technical Solution), and both Factors 1 and 2 being more important than Factor 3 (Technical Approach). Of the business factors, Factor 4 (Schedule) is more important than Factor 5 (Price). When combined, Factors 1, 2, and 3 are more important than Factors 4 and 5. Award shall be made to the Offeror whose quotation is determined to be the best value to the Government based on a tradeoff among the Technical and Business Factors.

| | |
|---|---|
| **Data Retention Requirements** | |
| DAT001 | System shall be able to retain data associated with activities for a minimum of 5 years |
| DAT002 | System shall be able to retain data associated with members for a minimum of 30 years after a member is no longer active |
| DAT003 | System shall be able to retain data associated with Auxiliary Facilities for a minimum of 2 years after it becomes inactive or is withdrawn from service |
| DAT004 | System shall be able to retain data associated with unit resources for a minimum of 5 years after final action is completed |
| DAT005 | System shall be able to retain data associated with the training management tool for a minimum of 30 years |
| DAT006 | System shall be able to retain reports for a minimum of 5 years |
| **Enterprise Architecture Requirements** | |
| EAR001 | Contractor shall provide a DoDAF Compliant: DIV-1 Conceptual Data Model |
| EAR002 | Contractor shall provide a DoDAF Compliant: DIV-2 Logical Data Model |
| EAR003 | Contractor shall provide a DoDAF Compliant: DIV-3 Physical Data Model |
| EAR004 | Contractor shall provide a DoDAF Compliant: SV-1 System Interface Description |
| EAR005 | Contractor shall provide a DoDAF Compliant: SV-2 System Resource Flow |
| EAR006 | Contractor shall provide a DoDAF Compliant: SV-6 System Resource Matrix |
| EAR007 | Contractor shall provide a DoDAF Compliant: STD-V1 Standards Profile |
| EAR008 | Provide an option to produce further DoDAF Compliant documentation as directed by the USCG. |
| **Cybersecurity Requirements** | |
| CYB001 | Infrastructure, Platform, and Software shall be compliant with FedRAMP+ Impact Level 4 as described in the DoD Cloud Computing SRG ver1, release 3. |
| CYB002 | System shall provide a Moderate level of Availability as defined in NIST federal policy. |
| CYB003 | Vendor shall produce reports and participate in events to validate the aforementioned security level. |
| CYB005 | Vendor shall ensure data is stored in physical locations where US federal laws apply. |
| CYB006 | Ensure all necessary CNSSI 1253 Privacy Overlays are implemented. |
| CYB007 | Vendor shall perform duties and responsibilities of the ISSO role as defined in the NIST Risk Management Framework and NIST Information Security Handbook. |
| CYB008 | Vendor shall work in concert with the USCG to attain a Provisional Authorization from DISA within 24 months of award. |
| CYB009 | Vendor shall adhere to the DoD CIO's memorandum dated 15NOV17, titled "Department of Defense Cybersecurity Activities Performed for Cloud Service Offerings" |

| | |
|---|---|
| CYB010 | Vendor shall be able to route all traffic through a DoD/USCG Cloud Access Point at the direction of the Government. |
| **Policy/Regulation Compliance Requirements** | |
| REG002 | Contractor shall comply with OMB Circular A-130 – Management of Federal Information Resources |
| REG003 | Contractor shall comply with Federal Information Security Management Act (FISMA) |
| REG005 | Contractor shall comply with Privacy Act of 1974 |
| REG006 | Contractor shall comply with Clinger-Cohen Act (CCA) |
| REG007 | Contractor shall comply with Department of Defense Instruction (DODI) 8510.01 Risk Management Framework (RMF) for DoD Information Technology (IT) |
| REG012 | Contractor shall comply with DHS 4300A – Sensitive Systems Handbook |
| REG013 | Contractor shall comply with NIST 800-53 (series) – Security and Privacy Controls for Federal Information Systems and Organizations |
| REG015 | Contractor shall comply with NIST 800-160 (series) – Systems Security Engineering |
| **Program Management Requirements** | |
| PM001 | Vendor shall conduct user support activities in alignment with support policy and documentation provided by the USCG. |
| PM002 | Vendor shall participate in weekly recurring meetings with the USCG to discuss performance, objectives, risks, schedules, and like concerns. |
| PM003 | Vendor shall provide reports based on the Cybersecurity Requirements on a monthly basis. |
| PM004 | Vendor shall provide montly service reports detailing the month's service metrics as compared to the service agreement. |
| PM005 | Vendor shall provide and execute a plan to return to agreed upon service levels in the event of a service breach as detailed by the service agreement. |
| PM006 | Vendor shall have a Service Management Plan. The service management plan shall include how the vendor will address Information Security Management, a Change Management Plan (design, develop, test, and deploy changes involving planned downtime, changes to system look, front end functionality, and/or cost shall be coordinated with the USCG), archive and searchable patch notes, Knowledge Management (e.g. desk guides, FAQs, user manuals, and/or training videos), participating in User Acceptance Testing, Service Continuity for unexpected loss or degradation of services, and the transition of the data back to the USCG at the conclusion of the contract. |
| PM007 | Vendor shall provide User Acceptance Testing plans and execute them for system changes involving modification to the look, front end functionality, and/or unplanned costs. |
| PM008 | If the vendor intends to deploy hardware to the field, the Service Management Plan shall include Supplier Management. |

**Attachment 6: AUXDATA STATEMENT OF WORK**
**RFQ 70Z0G319QPBZ02900**

# STATEMENT OF WORK
# FOR
# AUXDATA MODERNIZATION CALL

## 1.0 GENERAL

## 1.1 BACKGROUND.

The Auxiliary IT System (AUXDATA) is the United States Coast Guard's (USCG) only repository for personnel, program, and activity data for the Auxiliary's 25,700 active and 9,800 retired members who provide year-round high-quality support to virtually every USCG program. It is the platform for the Auxiliary Order Management System that is used to issue all Auxiliary patrol orders and facilitate the reimbursement of over $2.9M in associated Auxiliary patrol expenses (e.g., fuel, maintenance, meals). It is one of the Coast Guard's most heavily used information systems. Historically, it has been significantly underfunded. This funding deficit has resulted in a massive list of backlogged change requests needed to facilitate policy changes, as well as an inability to build additional functionality to properly track and manage new Auxiliary programs, such as Auxiliary Clergy Support (supporting CG-00A), Auxiliary Financial Educators (supporting CG-11 and CG-13), and the Auxiliary Build program (supporting CG-43). The government requires Contractor assistance transitioning the current AUXDATA system capabilities and its data to a Cloud-Hosted, vendor-managed Software-as-a-Service.

## 1.2 SCOPE.

This task order requires a rapid deployment of an AUXDATA system replacement. The purpose of the Auxiliary Data (AUXDATA) system can be summarized as follows:

- Accurately quantify the activities of the USCG Auxiliary members and produce a current record of those accomplishments in a variety of cumulative report formats.
- Provide up-to-date data and statistical information necessary to define the Auxiliary's mission value and position in the USCG family. Such information will be used by the USCG in presentations before the executive, legislative, and judicial branches of the Federal, State, and local Government agencies, as well as for intra- and inter-service and Public Affairs (media) needs.
- Provide an accurate depiction of Auxiliary member and facility capabilities to the Operational Commanders of the USCG needing or contemplating the use of the Auxiliary in accomplishing their missions.
- Maintain an automated national database for the Auxiliary organization with an ability to provide data reports at various organizational tiers.

## 1.3 REQUIREMENTS

The Contractor shall provide and implement a Commercial-off-the-shelf (COTS), Cloud-Hosted, Software-as-a-Service solution for the Government's AUXDATA system. The functional and non-functional requirements are attached in Appendix A. After implementation, there will be a transition phase where the Contractor will be required to transition all data (approximately 15GB of .dbf files stored in an Oracle 12c database), minimum 32,000 current users/accounts,

maximum 50,000 users/accounts, and train all end users on the Cloud-Hosted environment. Finally the Contractor shall provide regular maintenance and continued support. The purpose of the Auxiliary Data (AUXDATA) system application can be summarized as follows:

- Provide a means of access for Auxiliarist members and staff.
- Provide a means to manage all members of the Coast Guard Auxiliary.
- Provide a means to manage Auxiliary Organizational Units.
- Provide a means to track all activities of the Coast Guard Auxiliary.
- Provide a means to track resources of the Coast Guard Auxiliary.
- Provide a means to produce reports on all Coast Guard Auxiliary functions.
- Provide a means to manage training of Auxiliarists.
- Provide a means to manage security clearances of Auxiliarists.
- Provide a means to process patrol orders for the Coast Guard Auxiliary.

More detailed requirements can be found in Attachment 6/Appendix A.

**1.3 CONTRACTOR PERSONNEL.** The Contractor shall provide contracting support to deliver a fully operational and maintained solution in accordance with the requirements in this SOW and applicable Federal and Agency regulations.

**1.4 APPLICABLE BPA REQUIREMENTS.**

| | |
|---|---|
| 1.4.2 | Qualified Personnel |
| 1.4.3 | Employee Identification |
| 1.4.4 | Employee Conduct |
| 1.4.5 | Removing an Employee for Misconduct or Security Reasons |
| 1.4.6 | Conflict of Interest |
| 1.5 | SPECIAL REQUIREMENTS AND SECURITY |
| 1.6 | DEPARTMENT OF DEFENSE TRUSTED ASSOCIATE SPONSORSHIP SYSTEM (TASS) AND COMMON ACCESS CARDS |
| 1.7 | PLACE OF PERFORMANCE |
| 1.8 | HOURS OF OPERATION |
| 1.12 | PROTECTION OF INFORMATION |
| 1.13 | TRAVEL |
| 2.0 | GOVERNMENT FURNISHED PROPERTY/RESOURCES AND INFORMATION |
| 3.0 | CONTRACTOR FURNISHED PROPERTY |
| 4.1 | STATUS MEETINGS |
| 5.0 | REFERENCES |
| 6.0 | GOVERNMENT POINTS OF CONTACT |
| 7.0 | PAYMENT INFORMATION |
| 8.0 | CENTRALIZED INVOICE SUBMITTAL INSTRUCTIONS |

**1.5 PERIOD OF PERFORMANCE.** This call consists of a base period of one year, which includes implementation and management of the service, plus four one-year option periods for managing the service, for a total potential period of five years (60 months), if all options are exercised.

| | |
|---|---|
| Base Period: | 16 May 2019 – 15 May 2020 (12 Months) |
| Option Period 1: | 16 May 2020 – 15 May 2021 (12 Months) |
| Option Period 2: | 16 May 2021 – 15 May 2022 (12 Months) |
| Option Period 3: | 16 May 2022 – 15 May 2023 (12 Months) |
| Option Period 4: | 16 May 2023 – 15 May 2024 (12 Months) |

**1.6 CONTRACT TYPE.** CLINs for implementation and management of the service will be Firm-Fixed Price (FFP). CLINs for travel will be Time & Materials without G&A.

**1.7 DELIVERABLES AND REPORTING REQUIREMENTS.** See Section 5.0 below.

**2.0 DELIVERABLES**

**2.1 TECHNICAL/PROJECT DOCUMENTATION.** The Contractor shall provide the following documentation with the performance of this task order and as directed by the USCG:

| Item | Deliverable/Event | Description | Due By |
|---|---|---|---|
| **1** | Service Level Agreement (Draft) | Service Level Agreement between the Service Provider (Vendor) and Service Consumer (Government). This will be based upon the requirements in the call and various aspects of the proposal. The remaining aspects will be proposed by the vendor in this draft. The DHS standard SLA template will be utilized. | NLT Ten (10) business days after Call Award |
| **2** | Service Level Agreement (Final) | Service Level Agreement between the Service Provider (Vendor) and Service Consumer (Government). This will be the final version of the SLA, updated with the feedback from the Government on the SLA Draft, and signed by the Service Provider (Vendor). With Government approval, it will be signed and a copy returned to the vendor for their records. | NLT Twenty-Five (25) business days after award |

| | | | |
|---|---|---|---|
| **3** | Project Plan | The vendor project plan should include a work-breakdown structure and schedule for implementing the new solution, and transitioning data and operations from the current system to the new solution. Additionally, this plan should include the vendor's plan for conducting and recording user acceptance testing. | NLT Ten (10) business days after award |
| **4** | Training Plan (Draft) | The vendor must submit a proposed plan on how they will provide end-user training for all users of the new system | NLT Ten (10) business days after award |
| **5** | Training Plan (Final) | The vendor must submit its final plan and schedule for conducting end-user training. | TBD (dependent on proposed method and potential Government coordination) |
| **6** | Training Materials | Any proposed end-user training materials including but not limited to: videos, desk guides, course syllabi, power point presentations, etc. are subject to Government approval before dissemination. | TBD (dependent on proposed schedule and method) |
| **7** | User Acceptance Testing Report | Final report for completed user acceptance testing, verifying the solution is suitable for the end user. | TBD (dependent on proposed schedule) |
| **8** | Fully Operational Service | The point at which User Acceptance Testing is complete, all users and data have been transitioned to the system, the system is fully functioning, and services are being provided by the vendor. | TBD (dependent on proposed schedule) |
| **9** | Weekly Status Report | This weekly progress report shall include a summary of all Contractor work performed, all direct costs by line items, an assessment of technical progress, schedule status, any travel conducted and any Contractor concerns or recommendations for the period being reported that may impact successful Contractor | Weekly, every Wednesday from Call Award through transition to new solution |

| | | | |
|---|---|---|---|
| | | performance. | |
| **10** | Assist and develop ATO documentation | These documents are dictated by the National Institute of Science and Technology's Risk Management Framework. The contents of the deliverables will be provided jointly by the USCG and the vendor; however, the vendor will be responsible for producing many of the documents. The documents to be produced by the vendor will be detailed in the Security Plan of Actions and Milestones; which, is developed by the USCG. | In accordance with Security Plan of Actions and Milestones. |
| **11** | Monthly Service Metrics report | Report provides all pertinent service metrics as detailed in the vendor's Service Management Plan. This report must include the availability of services and the total unavailable minutes for all services delivered broken down between national day and night (Sunrise on East Coast to Sunset on West Coast) per the Requirements. | The first Friday of every month post implementation/transition |
| **12** | Monthly Incident and Problem Report | This report provides a summary of the events, incidents, and problems occurring within the month of report. An incident is an unplanned disruption of service(s) or an unplanned degradation to services. A problem is the root cause of one or more incidents. This report must include the total number of occurrences, average time to respond, and the number of repeat occurrences of Incidents and Problems during the period of report as well as all pertinent metrics as detailed in the vendor's Service Management Plan. | The first Friday of every month post implementation/transition |
| **13** | Knowledge Management Artifacts | These artifacts represent the knowledge management repository for the user base. The type of artifact (e.g. Desk Guides, FAQ's, and/or, Wiki, etc.) will depend upon the vendor's Service Management Plan. The content for these artifacts will come from | Upon identification by COR. |

| | | | |
|---|---|---|---|
| | | multiple sources such as user service requests, patch notes, incident/problem management, USCG management, etc. The vendor or the USCG can recommend new content; however, the content shall be developed by the vendor and approved for addition by the USCG. | |
| **16** | Patch Notes | Report that informs the user base of the changes they can expect to experience after the deployment of a new feature or update to the system. It also provides user with ancillary information to accompany a change (i.e. information not directly associated with the new/changed feature but pertinent for the user's ability to continue receiving the service from the tool). | Immediately following release of an update or new feature. |
| **17** | Transition Out | The Contractor shall assist the Government in transitioning data out of the system in the format it was transitioned in, or a format proposed by the Contractor that is acceptable to the Government. | Within 30 days of notification by COR. |

**2.2 POST-AWARD CONFERENCE.** The Contractor shall attend a Post-Award Conference with the Contracting Officer and the COR no later than five (5) business days after the call has been awarded. The purpose of the Post-Award Conference is to discuss technical and contracting objectives of the call. Within three business days post Post-Award Conference, the Contractor shall provide meeting minutes.

**2.3 WEEKLY STATUS REPORTS.** The Contractor shall provide a weekly status report to the COR and Contracting Officer via electronic mail from the first Wednesday post-award to when the transition to the new solution is complete. This weekly progress report shall include a summary of all Contractor work performed, an assessment of technical progress, schedule status, any travel conducted and any Contractor concerns or recommendations for the period being reported that may impact successful Contractor performance.

**2.4 GENERAL REPORT REQUIREMENTS.** The Contractor shall provide all written reports in electronic format with read/write capability using applications that are compatible with the Coast Guard Standard Workstation.

**2.5 TRAINING REQUIREMENTS.** The Contractor shall provide a means for training all end-users to ensure they understand all system functionality. At a minimum a basic user guide should be available for all users before transition.

**3.0 ENTERPRISE ARCHITECTURE REQUIREMENTS.** All solutions and services shall meet DHS Enterprise Architecture policies, standards, and procedures. Specifically, the contractor shall comply with the following DHS EA requirements:

- All developed solutions and requirements shall be compliant with the HLS EA
- All IT hardware and software shall be compliant with the HLS EA Technical Reference Model (TRM) Standards and Products Profile
- Contractor shall assist the Government in submitting description information for all data assets, information exchanges and data standards, whether adopted or developed, to the Enterprise Data Management Office (EDMO) for review, approval and insertion into the DHS Data Reference Model and Enterprise Architecture Information Repository.
- Development of data assets, information exchanges and data standards shall comply with the DHS Data Management Policy MD 103-01 and all data-related artifacts shall be developed and validated according to DHS data management architectural guidelines.
- The tool shall be IPv6 compliant per OMB Memorandum M-05-22, August 2, 2005 and as defined in the US. 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.

**3.1 Transitioning Out.** Throughout this call, the USCG is the sole owner of the data; both the data provided at the onset of the agreement and the data accrued and aggregated through the agreement's duration. At the end of the call the Government will require full cooperation in transitioning its data out of the Contractor system within 30 days of notification by the COR. At a minimum, the Contractor must be able to transition the data out of their system in the format it was transitioned in; however, the Contractor may propose alternative formats to transition the data that can be used with approval by the COR. Upon completion of the transition, the Contractor will attest, in writing, that its system no longer contains any of the data.

**3.2 Invoicing Payment Schedule**

Implementation/Transition Phase: This phase begins at call award and concludes upon the 'Fully Operational Service' Event. This phase is firm-fixed price and may only be invoiced after complete.

Service Management Phase: This phase begins after the 'Fully Operational Service' Event and continues through call expiration. This firm-fixed price phase includes a base period and four 12-month options. Each option price will be divided by the number of months in that period for equal firm-fixed monthly payments.

**APPENDIX A:**

**Attachment 6: AUXDATA STATEMENT OF WORK**
**RFQ 70Z0G319QPBZ02900**

Attachment 6
Appendix A.xlsx