DESCRIPTION/REQUIREMENTS/WORK STATEMENT

STATEMENT OF WORK (SOW)
FOR THE
AUTONOMOUS SURVEILLANCE TOWERS (AST) SYSTEMS

C.1 BACKGROUND

In support of the US Customs and Border Protection (CBP) mission of securing our nation's borders, CBP has a need to procure autonomous border surveillance capabilities. This capability will serve to enrich relevant CBP information technology systems of record by providing new data streams that support improved situational awareness to ongoing tactical operations and strategic support without requiring additional staffing resources to support.

In February 2019 CBP deployed [redacted] Autonomous Surveillance Towers in San Diego Sector (SDC) for a Pilot Program. Due to the success of the effort the CBP Innovation Team was given guidance to deploy additional autonomous surveillance capabilities. Following the pilot an additional [redacted] Towers were procured for deployment in SDC and Laredo (LRT) Sectors.

CBP Innovation Towers (INVNT) has determined that there are additional requirements to support multiple CBP customers via a contract award for Autonomous Surveillance Towers. CBP has a mission to monitor between ports of entry, maritime domains, and part-time ports of entry. The same family of technology capabilities were deployed along the southern border during the AST pilot deployment. Utilization of this technology in the CBP environment has the potential to enable CBP operators to carry out their mission more safely and effectively.

C.2 SCOPE

This Statement of Work (SOW) describes the installation, performance, evaluation, and logistical support requirements for the U.S. Customs and Border Protection (CBP) [redacted].

This SOW provides CBP with a contract vehicle to acquire, deploy, operate and sustain the autonomous surveillance capabilities necessary to fulfill operational requirements along the southern, northern, and maritime U.S. Borders. This contract allows for the procurement, sustainment, maintenance, test, deployment/re-deployment, modification and enhancement of this capability. In addition, this contract allows for Autonomous Surveillance Capabilities as a service as Mission requirements dictate.

The contractor shall have total program responsibility for ensuring that the requirements in this SOW and the AST Capability Requirements are met. The contractor shall provide

program management, engineering, procurement, fabrication, manufacturing, installation, integration, testing, deployment/re-deployment, enhancement and sustainment of all modifications for the AST.

1. Order of Precedence

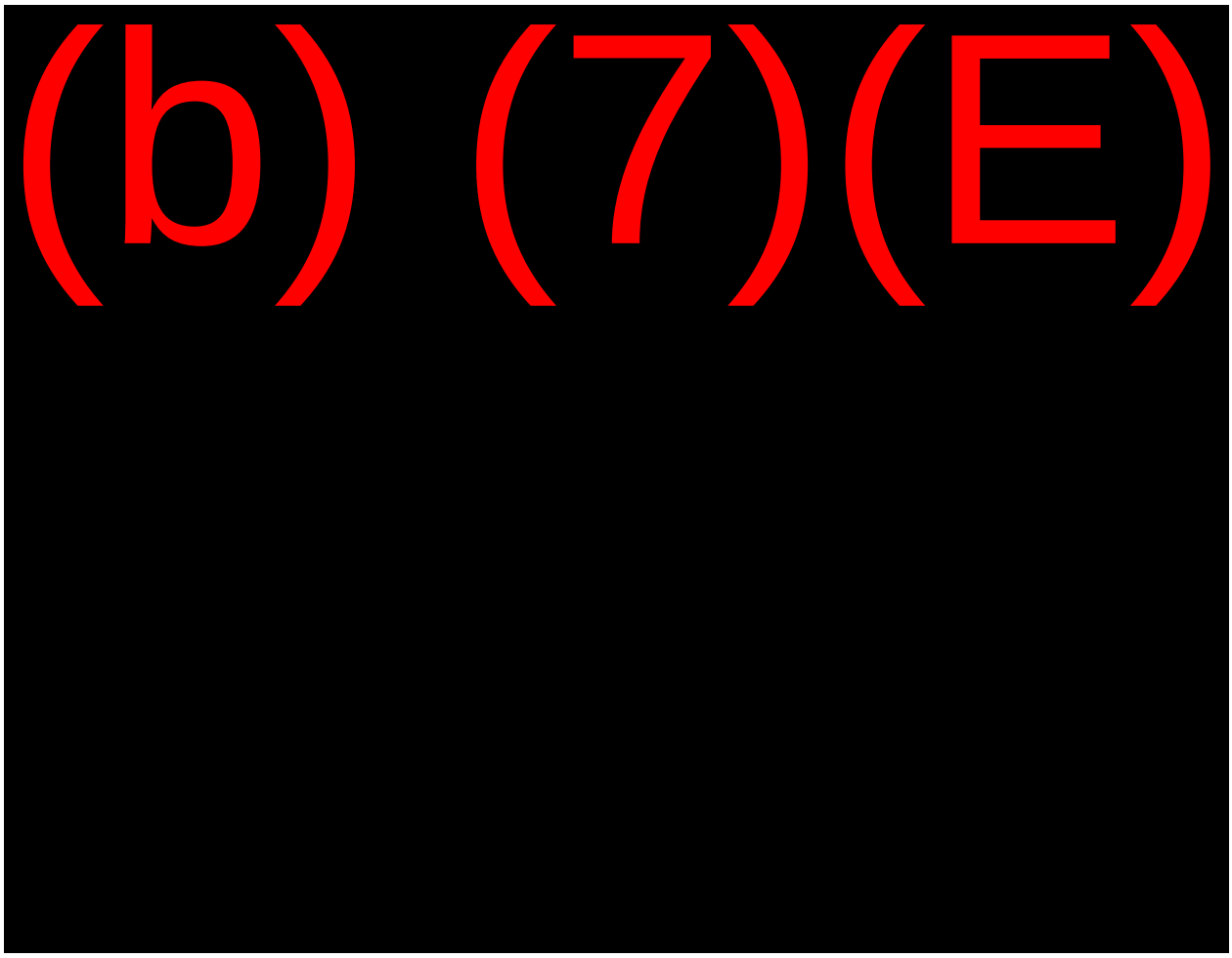
Throughout this SOW, the amendment or revision in effect as of the date of award shall apply. Where industry standards are referenced, the issue or revision in effect on the date of release of award shall apply. In case of inconsistency between the documents referenced herein, the following order of precedence applies:

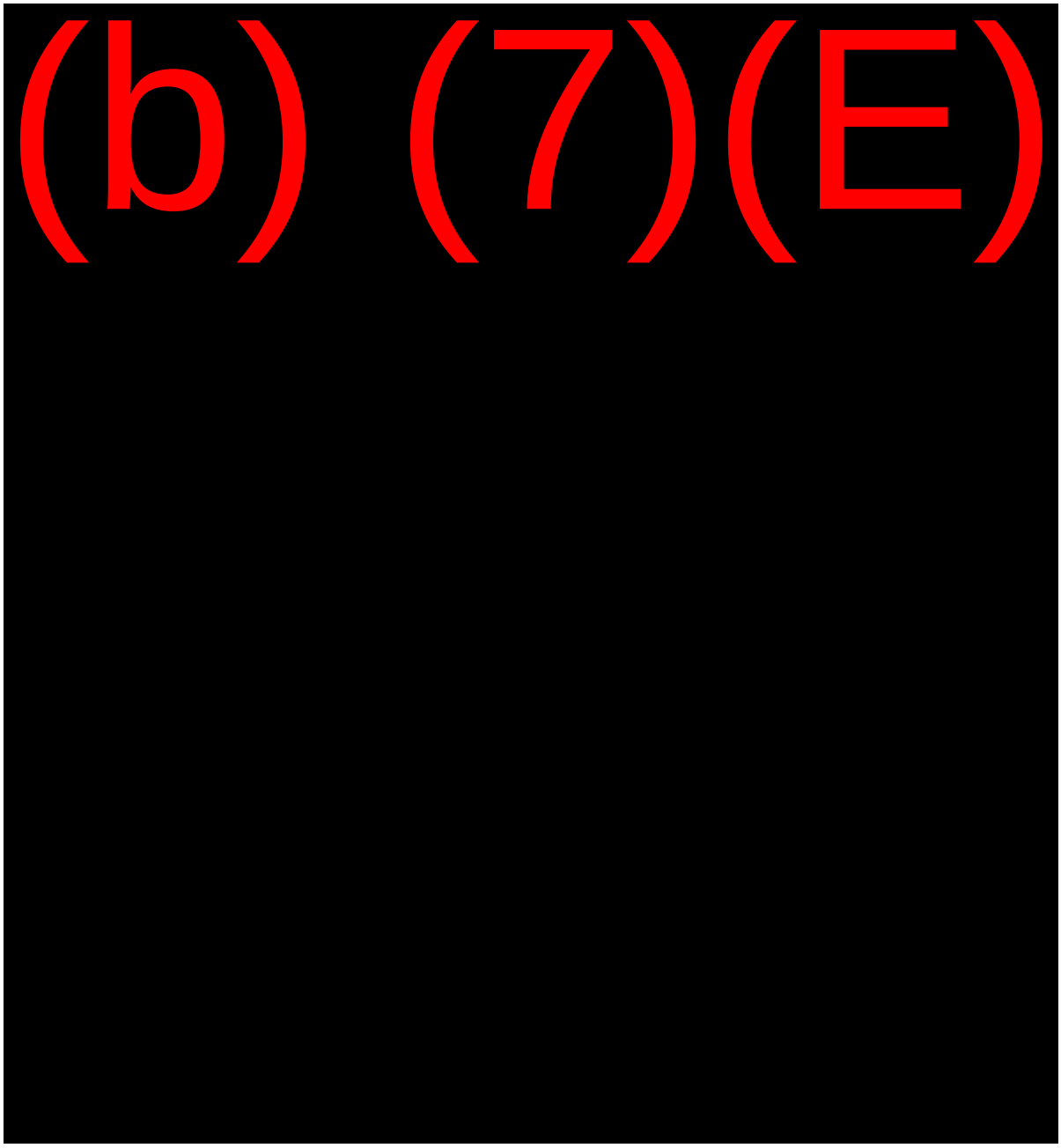
a. Contract requirements;

b. Capability Requirements; and

c. Government specifications and standards, industry standards, and similar referenced documents to include the DHS Acquisition Lifecycle Framework (ALF) and Systems Engineering Lifecycle (SELC)

C.3 GENERAL REQUIREMENTS





2. Materials

(a) <u>During the O&S period</u>

(b) 

At the end of the O&S period specified in each applicable task order (and provided the Government has not renewed or otherwise extended the O&S period) the system in the currently approved baseline to include all hardware, system and cloud software (not inclusive of source code), system and technical data shall be transitioned to the Government for ownership, operation and/or sustainment, according to a transition plan to be negotiated in good faith by the parties, 120 days prior to the end of the period of performance. The contractor shall, at the Government's request, work in good faith to provide input and assistance in determining the scope, nature, and cost of any such transition. Notwithstanding the foregoing, the contractor is not required to provide spare parts, software source code, hosting costs, communications costs, or ongoing services (including software updates) to sustain the capability beyond the O&S period specified in an applicable task order, except pursuant to a separate contract or task order as described in the transition plan to be mutually agreed by the parties.

3. Deployment/Re-Deployment

The Contractor shall perform all the necessary activities to complete a site-specific deployment or re-deployment of the procured system based on a Government notional laydown of each deployment location. The Contractor shall conduct a Deployment Readiness Review (DRR) 30 days prior to the deployment of the system at a Government provided facility or a Contractor facility.

4. Schedule and Deliverables

The contractor shall develop and maintain an integrated master schedule, which includes task and milestone identification for the work to be accomplished under this SOW, within 15 calendar days after delivery order award (CDRL A002).

(a.) Shipping Address

Shipping Address will be identified on each Delivery Order awarded under this IDIQ.

5. Program Management Plan and Monthly Reports

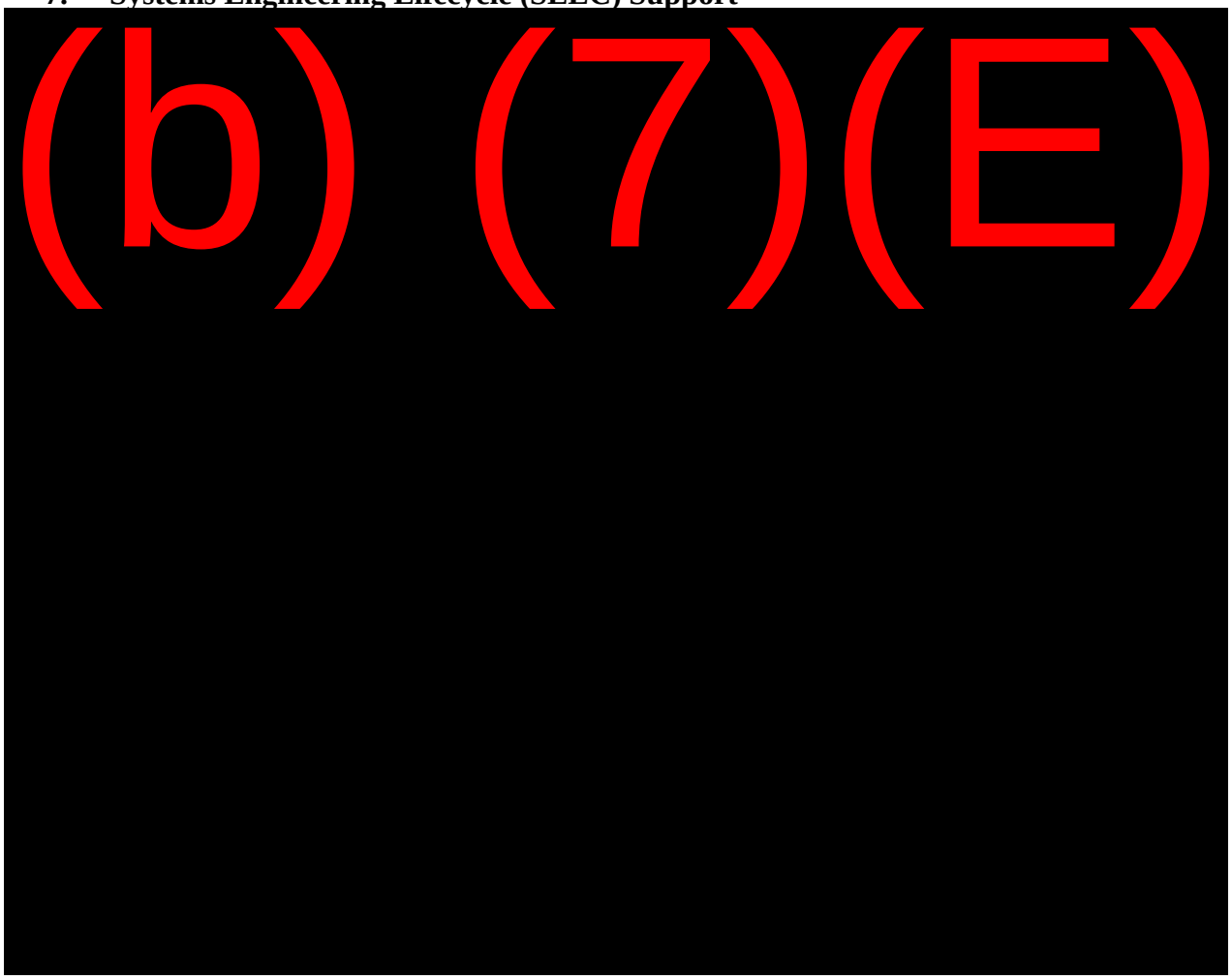
After the issuance of each delivery order, the contractor shall submit a Program Management Plan (CDRL A003). The contractor shall also submit monthly program, production and deployment progress reports to the Government (CDRL A004). The first monthly report is due no later than 30 calendar days from the date of order issuance and each report is due 30 calendar days thereafter until all AST systems are delivered to the Government. Those monthly reports shall provide sufficient information such as

financial status report, project progress and the status outline of each task; as well as reflect any task that is impacting a critical path against the delivery schedule.

6. Acquisition Lifecycle Framework (ALF) Support

The Program Management Office Directorate (PMOD) will complete the preliminary documentation to establish the Program of Record. Once the Program of Record is established, it is expected that the contractor will need to provide program and technical input for ALF documentation, including system performance metrics. The Contractor shall provide input sufficient to assist the Program Management Office in producing required Acquisition Documents. . This support is required to support the AST Program of Record documentation and major milestones post Acquisition Decision Event (ADE-3). Support will include, but not limited to input regarding enterprise architecture activities, technical insertion, post implementation reviews, operational analysis, and system performance metrics. The contractor shall provide program and technical input to support remediation of any ADE-3 Acquisition Decision Memorandum directions to PMOD.

7. Systems Engineering Lifecycle (SELC) Support



8. Quality System

The contractor shall maintain a quality system comparable to the most current and reasonably applicable requirements of ISO 9001 "Quality Systems - Model for Quality Assurance in Design, Development, Production, Installation, and Servicing," for the AST. All discrepancies reported by the Government shall be corrected 30 days prior to Government acceptance. The contractor shall provide their Quality Assurance Plan to the government within 30 days ARO (CDRL A005).

9. Existing Technical Solution

The AST shall be derived from existing technical solutions for autonomous surveillance capabilities deployed along the U.S. Border. Current production capabilities could satisfy all or part of the Capability Requirements.

10. Service Life

The AST system shall have a service life of at least five (5) years before requiring major overhaul or replacement, provided it is operated and sustained by the contractor during that period. The sensor payload should perform up to the specifications outlined in the relevant Capability Requirements for at least three (3) years before requiring system upgrades to remain current with commercial technology, provided it is operated and sustained by the contractor during that period.

11. Warranty

The workmanship, performance, and operation of each AST shall be warranted by the contractor against defects or failures, under the anticipated operating conditions as outlined in this capability requirement, for a period of one (1) year from the date of government acceptance (CDRL A006).

(a.) System Maintenance, Sustainment and Warranty Plan

The contractor shall be solely responsible for sustaining the system during the O&S period specified in each applicable task order. The contractor shall maintain all hardware and software components of the system in accordance with the requirements of the SOW. To the extent practicable, all hardware, software and operational capabilities shall continue to function in accordance with the requirements of the SOW at the end of the O&S period , independent of the Government's decision to purchase follow-on or additional support/maintenance. Notwithstanding the foregoing, the contractor is not required to provide spare parts, software source code, hosting costs, communications costs, or ongoing services (including software updates) to sustain the capability beyond the O&S period specified in an applicable task order, except pursuant to a separate contract or task order as described in the transition plan to be mutually agreed by the parties. (see Sec. 2(b), *supra*).

i. <u>Hardware</u>

During the O&S period specified in each applicable task order, the contractor shall keep the Government informed of all maintenance and sustainment actions that impact the

system's performance to include warranty information and warranty repairs by sending a monthly maintenance report. A summary of maintenance and warranty issues will include, at a minimum, the following items:

a. Date of report of claim;

b. Date of remediation;

c. Parts affected, including the system serial number (SN)

d. Nature of issue;

e. Actions taken; and

f. If issue is still open, intended action.

The contractor shall consolidate and analyze the hardware maintenance and repair data in a Monthly Maintenance Report, which analyzes maintenance and repair data to identify trends (CDRL A007). Additionally, hardware configuration changes shall be approved by the Government prior to any changes being made and documented in accordance with the configuration management (CM) process. The (CM) process will be shared with the contractor.

The Contractor will be given access to the Government provided Integrated Logistics Support System (ILSS) tool . All system maintenance data, tracking assets, inventory, procurements, metrics and related information will be tracked by the contractor's in-house serial and configuration management system. The contractor will send full serial and maintenance reports to the COR on a monthly basis or as requested. The Government will make ILSS training available to the Contractor online at no cost. All Contractor personnel shall obtain a final suitability clearance in accordance with DHS and CBP policies, procedures, and regulations to access ILSS.

In addition, the contractor shall provide an electronic record containing specific information for each AST including a list of all legacy AST assets that are currently being managed along with the end date of all warranty and support agreements. This includes, but is not limited to, all serial numbers for serialized components installed on a system that apply to the AST. Components and serial numbers are to be detailed in an Asset Management and Tracking Plan (CDRL A008).

Other Repairs are repairs that do not fall under the requirements of CMLS (e.g., due to incidents/accidents, acts of nature, sabotage, malicious damages, corrosion restoration, etc.). Upon request, the Contractor shall provide a quote for Other Repairs. The resulting quote shall be a Firm Fixed Price (FFP) quote for the Other Repairs (including all associated labor, travel, per diem, services, parts, and materials).

ii. Software

During the O&S period specified in each applicable task order, the contractor shall continuously update the system software to address deficiencies, add features and system enhancements, and to meet security requirements for continuous monitoring under the

National Institute of Standards and Technology (NIST) Risk Management Framework that are identified by the Government as applicable to the system. The contractor shall utilize commercial best practices for continuous software development, sustainment, operations, and security. These software processes and methodologies shall be documented in a Software Development Plan (CDRL A009) and approved by the government.

As part of the continuous software development, sustainment, operations and security process, the contractor shall maintain a product feature backlog which prioritizes all outstanding software feature requests, system improvements, deficiencies, and outstanding security requirements (CDRL A010). The process for managing the product feature backlog shall be detailed in the Software Development Plan. Software configuration changes shall be approved by the Government prior to any changes being made and documented in accordance with the configuration change process.

12. Operational Availability

The AST system is a necessary capability for the performance of the Border Security mission which is 24/7 operations 365 days a year. To meet CBP Operational Availability requirements, which will be provided for each delivery order based on the deployment requirements. The contractor shall be solely responsible during the O&S period for maintaining system operational availability. An operational mission failure is any hardware/software failure or fault that prevents the system from meeting the requirements in this performance Capability Requirement.

13. System Safety Requirements

The contractor shall maintain a system safety program, documented in the program management planning, that identifies significant hazards associated with the design of the AST and all deployed AST systems. The system safety program shall leverage or adapt processes consistent with MIL-STD-882E or any commercial equivalent. In addition, the contractor shall provide a methodology to either eliminate or control those hazards. Materials and processes shall, along with other design criteria, minimize environmental impacts from the manufacture, operation, maintenance, and repair of the AST and its subsystems as designed, deployed, and sustained. If requested, the contractor shall provide a Safety Assessment Report for all AST systems (CDRL A011).

14. Configuration Management Plan

The Contractor shall establish a Configuration Management Plan and maintain it throughout the life of this contract. The Contractor shall satisfy project objectives and meet the reasonably applicable requirements of ANSI/EIA-649 or other commercial best practices for configuration management, and the AST Capability Requirement (CDRL A012). The Configuration Management Plan must be approved by the government.

15. Software and Hardware Substitutions

During the O&S period specified in each applicable task order, the Contractor shall provide within scope nonrecurring engineering support for Government requirements for

engineering change proposals, engineering studies, and system analysis. Proposed system changes may be initiated either by request from the Government or recommendations made by the contractor. Any changes or modifications to the AST systems hardware and software will be communicated by the contractor to the Government for review and approval. Hardware and Software changes which enhance the system capability and/or reduce the system operational cost are highly desired and encouraged.

Hardware and software substitutions or configuration changes of items in subsequent systems shall be approved by the Government prior to any changes being made and documented in accordance with the configuration change process. The Contractor shall provide a proposal for hardware and software substitutions as they come up and will also address fielded legacy systems.

The Contractor shall document approved AST system baselines in a System Description Document (SDD) which captures Hardware, Software, and Network Description Information (CDRL A013). As new versions of the system are released/deployed they will be accompanied by a Version Description Document (VDD) (CDRL A014).

16. Government Furnished Equipment and Information:

Government Furnished Equipment and Information (GFE/GFI) List will be provided to the vendor at the award of each relevant delivery order.

C.4 TECHNICAL SUPPORT REQUIREMENTS

The contractor shall provide program, technical, manufacturing, engineering, and deployment liaison management. Access to production facilities, technical records, and system data shall be granted to Government representatives in accordance with the contract terms and conditions or upon mutual agreement of both parties. The contractor's program manager shall be the primary interface with the Government. The contractor shall report the current status of the AST project in a monthly progress report.

C.5 TRAINING

During the O&S period specified in each applicable task order, the contractor shall provide Operator Training on the System and User Interface (UI) for users at locations receiving AST systems. The training shall be designed so that users become familiar with the systems performance capabilities and limitations. Operator training may include classroom training, initial instruction, on-the-job training, refresher/new feature training, and train the trainer (T3). For select users, the training shall also include start-up and shut-down procedures; warnings; disassembly, packaging, safe relocation, reassembly, and emergency procedures, as applicable. Basic maintenance procedures and techniques may also be addressed, if applicable. The contractor shall deliver a training package for each AST system (CDRLA015). Detailed training requirements will be identified in each Delivery Order.

C.6 MAINTAINABILITY REQUIREMENTS

1. Preservation, Packaging and Packing of Parts and Tools

The Contractor shall inspect all material for damage, proper preservation, packaging, packing, and marking. Preservation, packaging, packing, and marking shall follow OEM requirements.

2. Logistics and Provisioning Data

The contractor shall provide provisioning technical data (PTD) that is required to purchase maintenance supplies, spare parts, and replacement parts over the lifecycle of the AST (CDRL A016). The contractor will brief the COR on significant logistics and supply chain changes and risks that will impact performance as part of its periodic briefings and provide an updated copy of the PTD upon request. The contractor shall brief the COR on any changes affecting equipment or parts configurations that will impact the performance of the contract during as part of periodic briefings. Upon government request, the contractor shall provide a revised PTD.

The PTD shall include:

A. Master equipment list;

B. List of special tools and test equipment; and

C. Long lead time parts list.

(a.) Master Equipment List

The contractor shall provide an indentured master equipment list that identifies all the parts that can be assembled, re-assembled, or replaced on the AST

(b.) Special Tools and Test Equipment

The contractor shall provide a list of special tools and test equipment.

(c.) Long Lead Time Parts List

The contractor shall provide a list of long lead time parts that require more than 90 days to acquire.

1. HelpDesk Support

During the O&S period specified in each applicable task order, the Contractor shall provide help desk technical support to operators at each deployment location. The Contractor shall provide a Monthly Activity Report that documents all Technical Support activities.

C.7 PROGRAM REVIEWS

The contractor shall conduct program reviews to provide the PM, CO, and COR with the information necessary to assess the progress and performance of the contractor with respect to the requirements stated in this SOW and the AST performance Capability Requirement.

1. Program Management Review

The contractor shall provide facilities for a requirements review (PMR) to accommodate approximately 10 Government personnel, within 30 days after each delivery order is awarded. The purpose of the PMR shall be to allow the contractor to discuss system requirements and present derived requirements along with testing, validation, and verification methods and to review the supply support requirements and deployment requirements. The contractor shall provide a copy of the proposed agenda at least 10 calendar days prior to the review; and the minutes and action items for the PMR within 10 calendar days after the review (CDRL A017).

2. Technical Reviews

Technical information meetings may be conducted to gain further clarification about the design of the AST, Deployment, Modifications/Enhancements, and System Sustainment. Meetings can be conducted telephonically or at the contractor's facility. Technical Review Meetings may be scheduled at the request of the government. At minimum, and unless otherwise requested by the Government, the contractor shall provide facilities for 2 day quarterly progress meetings to accommodate approximately 10 Government personnel during the term of the contract to review program status (CDRL A018).

C.8 INSPECTION, ACCEPTANCE & TESTING REQUIREMENTS

1. Inspection (Government Contract Quality Assurance)

During the performance of the contract, the contractor shall provide Government access to the manufacturing facility to perform quality assurance inspections. Quality assurance inspections are to be performed on all supplies or services to determine conformity to the contract requirements. Quality assurance inspections will take place at the source. Quality assurance inspections are in accordance with the Federal Acquisition Regulation (FAR) clause 52.246-2 Inspection of Supplies-Fixed Price.

2. Acceptance Inspection

The Government will perform a visual acceptance inspection of the AST Systems upon delivery and provide a detailed list of discrepancies within 10 business days to the contractor for resolution.

3. Test and Evaluation (T&E)

Acceptance testing shall commence and be performed by the government upon delivery to CBP. Upon delivery CBP will validate the adherence of AST Capability Requirement by the contractor. CBP will identify specific deployment locations for each Delivery Order awarded under this IDIQ. The contractor will assist the Government at no

additional cost in conducting one T&E for each AST model type deployed and/or for each deployment of the same AST model to a new operational environment (e.g., Northern Border, Southern Border, Maritime, etc.), as well as for required Cyber Testing.

The Government may execute additional Test and Evaluation (T&E) at its own cost, which will validate the AST Functional and Operational Requirements Documents. The Contracting Officer (CO) shall notify the Contractor in writing within 10 business days of the status of the approval or disapproval of delivery acceptance. This notification shall state any further action required of the Contractor for the current and subsequent deliveries. The contractor shall provide a Plan of Action and Milestones (POAM) with the path forward to address any discrepancies identified during acceptance and inspection.

T&E shall commence upon completion delivery order fielding. CBP may also conduct T&E throughout the lifecycle of the AST system at its own cost to validate the continued performance of the AST. The purpose of the T&E will be to determine if the AST is operationally suitable and ensure that it meets performance criteria outlined in CBP requirements documentation. T&E Documentation shall consist of, as applicable, the following documents (CDRL A019):

- Test Plans
- Test Procedures
- Test Readiness Reviews
- Quick Looks
- Test Reports

As an alternative to the T&E procedure described above, the Government may choose to perform T&E through a review of relevant performance metrics and service level agreements from the deployed AST in the relevant operational environment. Upon request, the contractor shall provide relevant metrics in a test report demonstrating the system is operationally suitable and meets performance criteria outlined in CBP requirements documentation.

C.9 TECHNICAL MANUALS, REPORTS, DATA AND DRAWINGS

The contractor shall provide technical manuals, reports, data, and drawings in accordance with the AST Capability Requirement. (CDRL A020).

The contractor shall provide all system operational data pursuant to the Government's instructions, including instructions pertaining to storage locations and retention limits (CDRL A021). System Data may include, but is not limited the following processed data:

- Imagery
- Radar Tracks
- Metadata, Health & Status
- User & Group Logs/System Admin
- Exclusion Zones
- Manual/Autonomous Control

- Usage Records
- Account Lists/Privileges
- Sensor Heading/Pointing Data.

C.10 PERFORMANCE PERIOD

The period of performance for this effort begins upon the date of award for five (5) years.

C.11 INVOICES

The contractor shall provide to the COR, electronic copy invoices with supporting documentation within 10 working days. The contractor shall identify the funding "breakout", on invoices by Line Item Number. The COR will review the delivered invoice within 5 business days of submission. After a review of the invoice by the COR, the invoice will be approved to submission to IPP.

ELECTRONIC INVOICING AND PAYMENT REQUIREMENTS - INVOICE PROCESSING PLATFORM (IPP) (JAN 2016)

Beginning April 11, 2016, payment requests for all new awards must be submitted electronically through the U. S. Department of the Treasury's Invoice Processing Platform System (IPP). Payment terms for existing contracts and orders awarded prior to April 11, 2016 remain the same. The Contractor must use IPP for contracts and orders awarded April 11, 2016 or later, and must use the non-IPP invoicing process for those contracts and orders awarded prior to April 11, 2016. "Payment request" means any request for contract financing payment or invoice payment by the Contractor. To constitute a proper invoice, the payment request must comply with the requirements identified in FAR 32.905(b), "Payment documentation and process" and the applicable Prompt Payment clause included in this contract. The IPP website address is: https://www.ipp.gov.

Under this contract/order, the following documents/information are required to be submitted with or as an attachment to the Contractor's payment request in IPP:

- Order number;
- Description of services provided for a specified time period;
- Unit price and total amount of each item;
- Discount terms;
- Company name, telephone number, taxpayer's identification number; and
- Complete mailing address to which payment will be mailed.

The IPP was designed and developed for Contractors to enroll, access and use IPP for submitting requests for payment. Contractor assistance with enrollment can be obtained by contacting IPPCustomerSupport@fms.treas.gov or phone (866) 973-3131.

If the Contractor is unable to comply with the requirement to use IPP for submitting invoices for payment, the Contractor must submit a waiver request in writing to the contracting officer.

C.12 PERSONNEL RESOURCES AND STAFFING

The contractor shall provide a list of names and proposed duties of the professional personnel, consultants, and subcontractor employees assigned to the project. Resumes for all individuals identified as "key personnel" shall be provided and shall include information on education, background, recent work experience, and specific scientific or technical accomplishments. The contractor shall provide an organization chart that clearly depicts the means of communication between its team members, management and subcontractors. The Contractor shall notify the Government of any changes to the organization (e.g. key personnel changes).

C.13 Policy

To the extent reasonably applicable to contractor's operations under this agreement or a relevant task order, the AST Systems must comply with the applicable standards and requirements from the following documents (see Table 1).

Table 1 – Policy

Nbr	Document
1	Security and Privacy Controls for Information Systems and Organizations. NIST Special Publication 800-53 standard current version.
2	System Reporting Form Standards for Security Categorization of Federal Information Processing Standards (FIPS 199)
3	DHS Standard 4300 A Sensitive Systems Policy current version.
4	DHS Directive (MD 11042.1) For Official Use Only (FOUO) Information" dated January 6, 2005
5	CBP Security Policy and Procedures Handbook (HB1400-05D), Current version, Volume IV, Chapter 13, FOUO Information
6	DHS Information Security Policy, identified in MD 4300.1, (IT) Systems Security Program and 4300A Sensitive Systems Handbook, current version
7	Section 508 of the Rehabilitation Act: http://www.section508.gov/
9	Security Guide for Interconnecting Information. NIST Special Publication 800-47 and DHS IT Security Policies
10	DHS Information Security Performance Plan (current version)
11	CBP Technical Reference Model (TRM) (current version)
12	DHS Security Operations Concept of Operation (current version)
14	Federal Information Security Management Act (Public Law 113-283).
15	ANSI/ISO/ASQ Q10007 – Quality Management Systems – Guidelines for Configuration Management
16	Information Security Continuous Monitoring. NIST Special Publication 800-137.
17	Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy. NIST Special Publication 800-37.

18	CBP Directive Operational Materiel Cost Wise Readiness (CWR) Policy and Oversight
19	DOD Reliability, Availability, Maintainability, and Cost Rationale Report Manual
20	Guide to LTE Security. NIST Special Publication 800-187
21	Protecting Controlled Unclassified. NIST Special Publication 800-171
22	Policy Memorandum: DHS Information System Configuration Standards
23	CBP Information System Security and Privacy Requirements
24	Department of Homeland Security and U.S. Customs and Border Protection Systems Policy Memoranda
25	Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIG)
26	DHS Instruction 102-01-001, Revision 01 Acquisition Management Instruction, May 5, 2019

C.14 Security

The following are a list of security requirements for the AST System and contractors.

CBP Systems are required to be configured securely and in accordance with approved configuration standards. The contractor shall follow all reasonably applicable DISA STIGs, DHS configuration guidelines, and other reasonably applicable industry recognized guides as the approved configuration standards for DHS information systems. The contractor shall support the mitigation of Plan of Action and Milestones (POAM) findings with the path forward to address any discrepancies identified during acceptance and inspection.

The Contractor shall provide system technical information to support obtaining Assessment and Authorization (A&A) to operate. The Government will conduct a Security Assessment and produce a Security Assessment Report (SAR) which will be provided to the Contractor. The Contractor shall provide operational and technical support to the Government during the Security Assessment event.

Table 2 contains security document requirements which, and only to the extent such requirements are reasonably applicable to the contractor's operations under this agreement or a relevant task order, the Contractor must complete for the AST system prior to connection to CBP's OneNet (CDRL A022).

Table 2 – NIST RMF Security Documents	
Security Requirement Document	**Comment**
System Security Plan (SSP)	Vendor Support as required
Security Requirements Traceability Matrix	Vendor Support as required
Contingency Plan	Vendor Support as required

Contingency Plan Test	Vendor Support as required
Input to US BP's Security Risk Assessment System	Vendor support as required
Security Assessment Plan	Vendor Support as required
Security Assessment Checklist	Vendor support as required
Provide any unique Memorandum of Understanding (MOU's)/Memorandum of Agreement (MOA's)/ Interconnection Security Agreement's(ISAs))	Vendor support as required
Security Test and Evaluation Network/System Scans using scanning tools compliant with current DHS policy.	Vendor support as required
Plan of Action & Milestones (POA&Ms) for any identified weaknesses	Vendor support is required
Vulnerability Scan Findings/POA&M Remediation Plans	Vendor support is required
Security Incident Report	Vendor support and interaction required
System Definition Workbook (template provide by GOVT)	Vendor support as required

The Contractor shall apply the DHS hardening guidance to the greatest extent possible without affecting the performance of the system. The Contractor shall install the latest patches, upgrades, and updates as well as the latest files (e.g., anti-malware definition files, configuration files, etc.) on a quarterly basis.

The Contractor shall perform vulnerability scans using Tenable Nessus or other OIT approved cybersecurity tools with the latest plugins and properly configured scan profiles every 30 days on the version of the software deployed on each system. The Government will provide assistance to ensure that the scan profiles contain credentials for all IP addressable devices that have credentials as well as DHS provided audit files for all Operating Systems (OSs).

The Contractor shall remediate all vulnerabilities (via configuration, removal, mitigation or update) ranked as high or critical within 30 days of detection/notification and all vulnerabilities within 180 days of detection/notification. The Contractor shall identify vulnerabilities through Tenable Nessus security scans or other approved tools and Government provided Information Security Vulnerability Management (ISVM) bulletins. The Contractor shall provide a monthly Tenable Nessus or equivalent scan report (CDRL A023).

Additional Security requirements can be found in the Security Clauses section of the contract.

C.15 Deliverables

The Contractor must provide deliverables in electronic format via email or other digital delivery method. Deliverables must be emailed to the COR and other designated representatives when feasible. Specific internet addresses for electronic submission of deliverables will be provided by the COR.

Applicable FOUO deliverables and otherwise sensitive documentation will be electronically submitted in a secure manner, encrypted and by signed email. The following deliverable time frames must be followed, at a minimum, unless otherwise agreed upon between the COR and the Contractor.

CDRLs require GOVT approval/disapproval. GOVT must have ten (10) working days to respond to the CDRL, or other document submittal; if no disapproval is received by contractor during this period, the submittal is considered accepted. CDRL 'due dates' are calendar dates (due dates on weekends, Gov't holiday will be delivered following business day). All CDRL deliveries must be provided electronically.

CDRL Number	**Title**	**SOW Section**	**Initial Delivery in Business Days**	**Frequency**
A001	Anduril Systems and Software		As Requested, At the end of the contract period of performance	Once
A002	Integrated Master Schedule		30 days after post-award conference	Updated as Requested
A0023	Project Management Plan (PMP)		With proposal bid	Updated as Requested
A004	Monthly Program Management Report (PMR)		30 days after post-award conference	Monthly
A005	Quality Assurance Plan		30 days after post-award conference	updated as requested
A006	Warranty Information		30 days after post-award conference	Updated as Requested
A007	Monthly Maintenance Report		30 days after post-award conference	Monthly

A008	Asset Management and Tracking Plan		30 days after post-award conference	Updated as Requested
A009	Software Development Plan		30 days after post-award conference	Updated as Requested
A010	Product Feature Backlog		30 days after post-award conference	Updated as defined in the Software Development Plan
A011	Safety Assessment Report (SAR)		As requested	Updated as Requested and as System Changes are Implemented
A012	Configuration Management Plan		30 days after post-award conference	Updated 30 days prior to ATO anniversary date
A013	System Description Document (SDD)		90 days after contract award	As required
A014	Version Description Document (VDD)		90 days after contract award	As required
A015	Training Materials for operational, system administration, and maintenance (including tear down and reassembly for relocation) training material and sessions		10 days prior to training session	As required
A016	Logistics and Provisioning Data		30 days after post-award conference	Upon request
A017	Program Management Reviews		Within 30 days of Delivery Order Award	As required
A018	Technical Reviews		Quarterly, As Required	

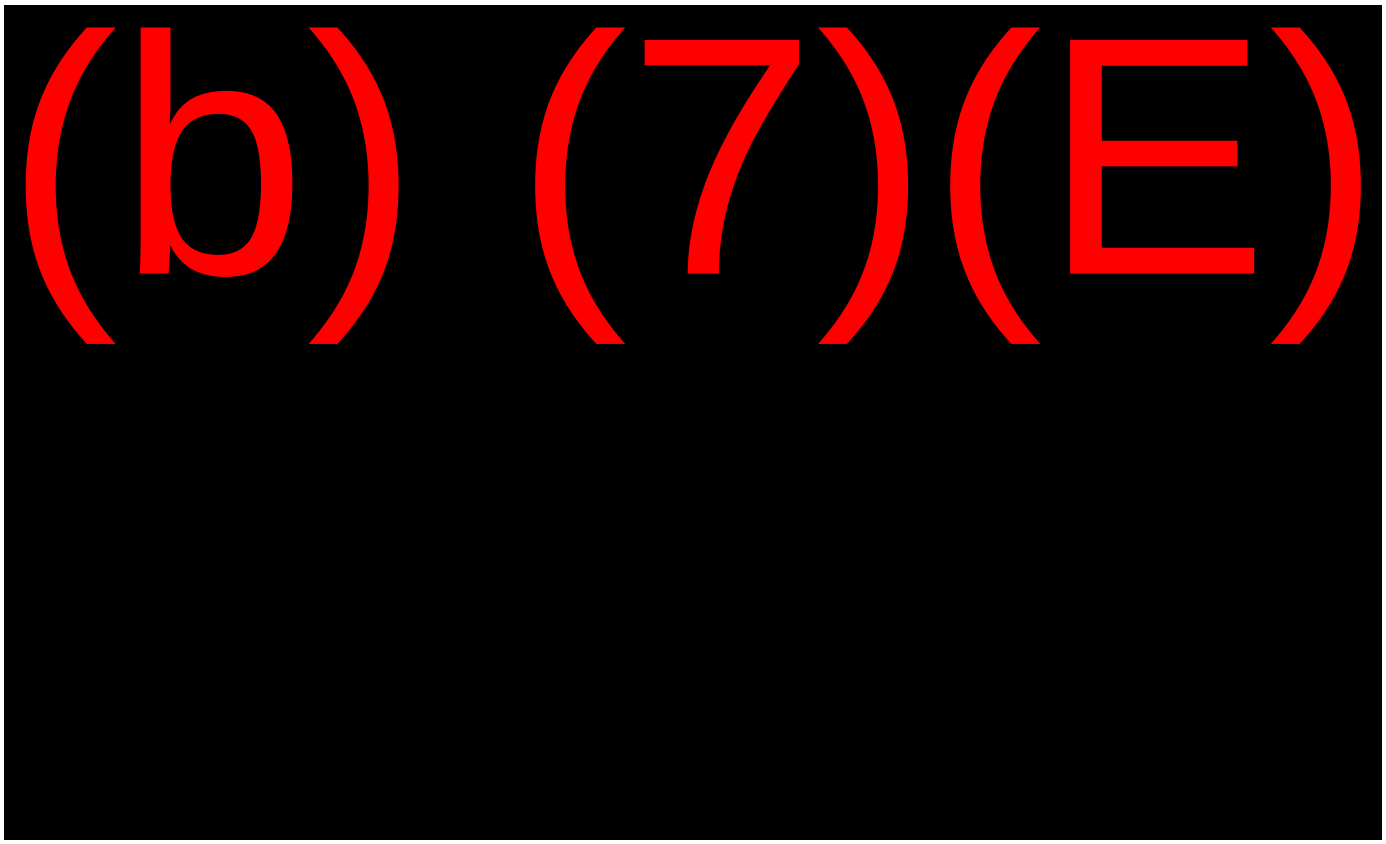
A019	Test Documentation

	Test Plan		30 days prior to SAT	As required
	Test Procedures		10 days prior to SAT	As required
	Test Readiness Review (TRR)		10 days prior to SAT	As required
	Quick Look		Quick Look 5 days after SAT	As required
	Test Report		Final due 30 days after SAT	As required
A020	Technical Manuals (Operations and Maintenance), reports, data, and drawings		90 days after Delivery Order Award	Updated as required
A021	System Operational Data		As Requested, At the end of the contract PoP or as otherwise instructed.	
A022	NIST RMF Security Documents		60 days prior to SAT	Updated 30 days prior to ATO anniversary date
A023	Vulnerability Scans		Within 30 days of delivery order award	Monthly, As requested
A024	Security Plan		60 days prior to SAT	As requested

C.16 Travel

Travel may be required for the performance of this contract. Specific trips associated with this contract shall be undertaken only with the advance written approval of the COR. Approvals for travel may be requested on the basis of a particular task or sub-task as logical for performance under the contract. Travel costs shall comply with contract term H.3, *Travel Costs*. No indirect costs, G&A, or Fee shall be applied to Travel costs except for standard booking or reservation charges. The Government will not reimburse any travel expenses that are not within the rates of the Federal Travel Regulation (FTR).

C.17 Image Labeling



C.18 TERMS AND CONDITIONS

I.1 52.232-39 UNENFORCEABILITY OF UNAUTHORIZED OBLIGATIONS (JUN 2013)

(a) Except as stated in paragraph (b) of this clause, when any supply or service acquired under this contract is subject to any End User License Agreement (EULA), Terms of Service (TOS), or similar legal instrument or agreement, that includes any clause requiring the Government to indemnify the Contractor or any person or entity for damages, costs, fees, or any other loss or liability that would create an Anti-Deficiency Act violation (31 U.S.C. 1341), the following shall govern:

(1) Any such clause is unenforceable against the Government.

(2) Neither the Government nor any Government authorized end user shall be deemed to have agreed to such clause by virtue of it appearing in the EULA, TOS, or similar legal instrument or agreement. If the EULA, TOS, or similar legal instrument or agreement is invoked through an "I agree" click box or other comparable mechanism (e.g., "click-wrap" or "browse-wrap" agreements), execution does not bind the Government or any Government authorized end user to such clause.

(3) Any such clause is deemed to be stricken from the EULA, TOS, or similar legal instrument or agreement.

(b) Paragraph (a) of this clause does not apply to indemnification by the Government that is expressly authorized by statute and specifically authorized under applicable agency regulations and procedures.

I.2 3052.205-70 ADVERTISEMENTS, PUBLICIZING AWARDS, AND RELEASES (SEP 2012) ALTERNATE I (SEP 2012)

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

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

(End of clause)

I.3 3052.212-70 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 are incorporated by reference:

[The Contracting Officer should either check the provisions and clauses that apply or delete the provisions and clauses that do not apply from the list. The Contracting Officer may add the date of the provision or clause if desired for clarity.]

(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 Protege Program.

(b) Clauses.

[ ] 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.
[ ] Alternate I

[X] 3052.205-70 Advertisement, Publicizing Awards, and Releases. [ ] 3052.209-73 Limitation on Future Contracting. [ ] 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.
[ ] 3052.219-70 Small Business Subcontracting Plan Reporting. [ ] 3052.219-71 DHS Mentor Protege Program.
[ ] 3052.228-70 Insurance.

[ ] 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.
[ ]

Altern ate I [
]

Altern ate II
[ ] 3052.247-71 F.o.B. Origin Only.

[X] 3052.247-72 F.o.B. Destination Only.

(End of clause)

I.4 52.224-3 PRIVACY TRAINING, ALTERNATE I (DEVIATION)

(a) Definition. As used in this clause, personally identifiable information means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. (See Office of Management and Budget (OMB) *Circular A-130, Managing Federal Information as a Strategic Resource*).

(b) The Contractor shall ensure that initial privacy training, and annual privacy training thereafter, is completed by contractor employees who--

(1) Have access to a system of records;

(2) Create, collect, use, process, store, maintain, disseminate, disclose, dispose, or otherwise handle personally identifiable information on behalf of an agency; or

(3) Design, develop, maintain, or operate a system of records (see also FAR subpart 24.1 and 39.105).

(c) The contracting agency will provide initial privacy training, and annual privacy training thereafter, to Contractor employees for the duration of this contract. Contractor employees shall satisfy this requirement by completing *Privacy at DHS: Protecting Personal Information* accessible at http://www.dhs.gov/dhs-security-and-training- requirements- contractors. Training shall be completed within 30 days of contract award and be completed on an annual basis thereafter not later than October 31st of each year.

(d) The Contractor shall maintain and, upon request, provide documentation of completion of privacy training to the Contracting Officer.

(e) The Contractor shall not allow any employee access to a system of records, or permit any employee to create, collect, use, process, store, maintain, disseminate, disclose, dispose or otherwise handle personally identifiable information, or to design, develop, maintain, or operate a system of records unless the employee has completed privacy training, as required by this clause.

(f) The substance of this clause, including this paragraph (f), shall be included in all subcontracts under this contract, when subcontractor employees will -

(1) Have a system of records;

(2) Create, collect, use, process, store, maintain, disseminate, disclose, dispose or otherwise handle personally identifiable information; or

(3) Design, develop, maintain, or operate a system of records.

(End of clause)

I.5 PERIOD OF PERFORMANCE (MAR 2003)

The period of performance of this contract shall be from 05/01/2020 – 04/30/2025 inclusive of the base period and option periods.

[End of Clause]

I.6 TERM OF CONTRACT WITH OPTION(S) (ALTERNATE I) (MAR 2003)

The contract term shall consist of a 12-month base period and four (4) 12-month option periods as follows:

Base Period:	05/01/2020 – 04/30/2021
Option Year 1:	05/01/2021 – 04/30/2022
Option Year 2:	05/01/2022 – 04/30/2023
Option Year 3:	05/01/2023 – 04/30/2024
Option Year 4:	05/01/2023 – 04/30/2025

[End of Clause]

I.7 OPTION TO EXTEND THE TERM OF THE CONTRACT (MARCH 2000)

(a) The Government may extend the term of this contract by written notice to the Contractor within 30 days of expiration of the period of performance; provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least 60 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 5 years.

[End of Clause]

I.8 CONTRACTING OFFICER'S AUTHORITY (MAR 2003)

The Contracting Officer is the only person authorized to approve changes in any of the requirements of this contract. In the event the Contractor effects any changes at the direction of any person other than the Contracting Officer, the changes will be considered to have been made without authority and no adjustment will be made in the contract price to cover any increase in costs incurred as a result thereof. The Contracting Officer shall be the only individual authorized to accept nonconforming work, waive any requirement of the contract, or to modify any term or condition of the contract.
The Contracting Officer is the only individual who can legally obligate Government funds. No cost chargeable to the proposed contract can be incurred before receipt of a fully executed contract or specific authorization from the Contracting Officer.

[End of Clause]

I.9 ELECTRONIC INVOICING AND PAYMENT REQUIREMENTS - INVOICE PROCESSING PLATFORM (IPP) (JAN 2016)

Beginning April 11, 2016, payment requests for all new awards must be submitted electronically through the U. S. Department of the Treasury's Invoice Processing Platform System (IPP). Payment terms for existing contracts and orders awarded prior to April 11, 2016 remain the same. The Contractor must use IPP for contracts and orders awarded April 11, 2016 or later, and must use the non-IPP invoicing process for those contracts and orders awarded prior to April 11, 2016. "Payment request" means any request for contract financing payment or invoice payment by the Contractor. To constitute a proper invoice, the payment request must comply with the requirements identified in FAR 32.905(b), "Payment documentation and process" and the applicable Prompt Payment clause included in this contract. The IPP website address is: https://www.ipp.gov.Under this contract, the following documents are required to be submitted as an attachment to the IPP*: NIA*
The IPP was designed and developed for Contractors to enroll, access and use IPP for submitting requests for payment. Contractor assistance with enrollment can be obtained by contacting IPPCustomerSupport@fms.treas.gov or phone (866) 973-3131.
If the Contractor is unable to comply with the requirement to use IPP for submitting invoices for payment, the Contractor must submit a waiver request in writing to the contracting officer.
(End of Clause)

I.10 GOVERNMENT CONSENT OF PUBLICATION/ENDORSEMENT (MAR 2003)

Under no circumstances shall the Contractor, or anyone acting on behalf of the Contractor, refer to the supplies, services, or equipment furnished pursuant to the provisions of this contract in any news release or commercial advertising without first obtaining explicit written consent to do so from the Contracting Officer

The Contractor agrees not to refer to awards in commercial advertising in such a manner as to state or imply that the product or service provided is endorsed or preferred by the Federal Government or is considered by the Government to be superior to other products or services.

[End of Clause]

I.11 SECURITY PROCEDURES (OCT 2009)

A. Controls

1. The Contractor shall comply with the U.S. Customs and Border Protection (CBP) administrative, physical and technical security controls to ensure that the Government's security requirements are met.

2. All Government furnished information must be protected to the degree and extent required by local rules, regulations, and procedures. The Contractor shall comply with all security policies contained in CBP Handbook 1400-05D, c.7.0m Information Systems Security Policies and Procedures Handbook.

3. All services provided under this contract must be compliant with the Department of Homeland Security (DHS) information security policy identified in DHS Sensitive Systems Policy Directive 4300A, v.13.1, and DHS 4300A, v 12.0 or latest available version.

4. All Contractor employees under this contract must wear identification access badges when working in CBP facilities. Prior to Contractor employees' departure/separation, all badges, building passes, parking permits, keys and pass cards must be given to the Contracting Officer's Technical Representative (COTR). The COTR will ensure that the cognizant Physical Security official is notified so that access to all buildings and facilities can be revoked. NOTE: For contracts within the National Capitol Region (NCR), the Office of Internal Affairs, Security Management Division (IA/SMD) should be notified if building access is revoked.

5. All Contractor employees must be registered in the Contractor Tracking System (CTS) database by the Contracting Officer (CO) or COTR. The Contractor shall provide timely start information to the CO/COTR or designated government personnel to initiate the CTS registration. Other relevant information will also be needed for registration in the CTS database such as, but not limited to, the contractor's legal name, address, brief job description, labor rate, Hash ID, schedule and contract specific information. The CO/COTR or designated government personnel shall provide the Contractor with instructions for receipt of CTS registration information. Additionally, the CO/COTR shall immediately notify IA/SMD of the contractor's departure/separation.

6. The Contractor shall provide employee departure/separation date and reason for leaving to the CO/COTR in accordance with CBP Directive 1210-007A, Tracking of Contracting Employees. Failure by the Contractor to provide timely notification of employee departure/separation in accordance with the contract requirements shall be documented and considered when government personnel completes a Contractor Performance Report (under Business Relations) or other performance related measures.

B. Security Background Investigation Requirements

1. In accordance with DHS Instruction 121-01-007-01, Rev. 01, The Department of Homeland Security Personnel Security, Suitability and Fitness Program, Chapter 2, Personnel Security Program Standards, §13. Citizenship Requirements, contractor employees who require access to sensitive information must be U.S. citizens or have Lawful Permanent Resident (LPR) status. § 13E. A waiver may be granted, as outlined in in Chapter 2, § 14 of DHS Instruction Handbook 121-01-007-01.

2. Contractor employees that require access to DHS IT systems or development, management, or maintenance of those systems must be U.S. citizens in accordance with Chapter 2, Personnel Security Program Standards, § 13. Citizenship Requirements. § 13F. (Lawful Permanent Resident status is not acceptable in this case). A waiver may be granted, as outlined in Chapter 2, § 14 of DHS Instruction 121-01-007-01.

3. Provided the requirements of DHS Instruction Handbook 121-01-007-01 are met as outlined in paragraph 1, above, contractor employees requiring access to CBP facilities, sensitive information or information technology resources are required to have a favorably adjudicated background investigation (BI) or a single scope background investigation (SSBI) prior to commencing work on this contract. Exceptions shall be approved on a case-by-case basis with the employee's access to facilities, systems, and information limited until the Contractor employee receives a favorably adjudicated BI or SSBI. A favorable adjudicated BI or SSBI shall include various aspects of a Contractor employee's life, including employment, education, residences, police and court inquires, credit history, national agency checks, and a CBP Background Investigation Personal Interview (BIPI).

4. The Contractor shall submit within ten (10) working days after award of this contract a list containing the full name, social security number, place of birth (city and state), and date of birth of employee candidates who possess favorably adjudicated BI or SSBI that meets federal investigation standards. For employee candidates needing a BI for this contract, the Contractor shall require the applicable employees to submit information and documentation requested by CBP to initiate the BI process.

5. Background Investigation information and documentation is usually submitted by completion of standard federal and agency forms such as Questionnaire for Public Trust and Selected Positions or Questionnaire for National Security Positions; Fingerprint Chart; Fair Credit Reporting Act (FCRA) form; Criminal History Request form; and Financial Disclosure form. These forms must be submitted to the designated CBP official

identified in this contract. The designated CBP security official will review the information for completeness.

6. The estimated completion of a BI or SSBI is approximately sixty (60) to ninety (90) days from the date of receipt of the properly completed forms by CBP security office. During the term of this contract, the Contractor is required to provide the names of contractor employees who successfully complete the CBP BI or SSBI process. Failure of any contractor employee to obtain and maintain a favorably adjudicated BI or SSBI shall be cause for dismissal. For key personnel, the Contractor shall propose a qualified replacement employee candidate to the CO and COTR within 30 days after being notified of an unsuccessful candidate or vacancy. For all non-key personnel contractor employees, the Contractor shall propose a qualified replacement employee candidate to the COTR within 30 days after being notified of an unsuccessful candidate or vacancy. The CO/COTR shall approve or disapprove replacement employees. Continuous failure to provide contractor employees who meet CBP BI or SSBI requirements may be cause for termination of the contract.

C. Security Responsibilities

1. The Contractor shall ensure that its employees follow the general procedures governing physical, environmental, and information security described in the various DHS CBP regulations identified in this clause. The contractor shall ensure that its employees apply proper business practices in accordance with the specifications, directives, and manuals required for conducting work under this contract. Applicable contractor personnel will be responsible for physical security of work areas and CBP furnished equipment issued under this contract.

2. The CO/COTR may require the Contractor to prohibit its employees from working on this contract if continued employment becomes detrimental to the public's interest for any reason including, but not limited to carelessness, insubordination, incompetence, or security concerns.

3. Work under this contract may require access to sensitive information as defined under Homeland Security Acquisition Regulation (HSAR) Clause 3052.204-71, Contractor Employee Access, included in the solicitation/contract. The Contractor shall not disclose, orally or in writing, any sensitive information to any person unless authorized in writing by the CO.

4. The Contractor shall ensure that its employees who are authorized access to sensitive information, receive training pertaining to protection and disclosure of sensitive information. The training shall be conducted during and after contract performance.

5. Upon completion of this contract, the Contractor shall return all sensitive information used in the performance of the contract to the CO/COTR. The Contractor shall certify, in writing, that all sensitive and non-public information has been purged from any Contractor-owned system.

D. Notification of Contractor Employee Changes

1. The Contractor shall notify the CO/COTR via phone, facsimile, or electronic transmission, immediately after a personnel change become known or no later than five (5) business days prior to departure of the employee. Telephone notifications must be immediately followed up in writing. Contractor's notification shall include, but is not limited to name changes, resignations, terminations, and reassignments to another contract.

2. The Contractor shall notify the CO/COTR and program office (if applicable) in writing of any proposed change in access requirements for its employees at least fifteen (15) days, or thirty (30) days if a security clearance is to be obtained, in advance of the proposed change. The CO/COTR will notify the Office of Information and Technology (OIT) Information Systems Security Branch (ISSB) of the proposed change. If a security clearance is required, the CO/COTR will notify IA/SMD.

E. Non-Disclosure Agreements

When determined to be appropriate, Contractor employees are required to execute a non-disclosure agreement (DHS Form 11000-6) as a condition to access sensitive but unclassified information.

[End of Clause]

I.12 NON-PERSONAL SERVICE (MAR 2003)

1. The Government and the contractor agree and understand the services to be performed under this contract are non- personal in nature. The Contractor shall not perform any inherently Governmental functions under this contract as described in Office of Federal Procurement Policy Letter 92-1

2. The services to be performed under this contract do not require the Contractor or his employees to exercise personal judgment and discretion on behalf of the Government, but rather, the Contractor's employees will act and exercise personal judgment and discretion on behalf of the Contractor.

3. The parties also recognize and agree that no employer-employee relationship exists or will exist between the Government and the Contractor. 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:

(a) Be placed in a position where there is an appearance that they are employed by the Government or are under the supervision, direction, or evaluation of any Government employee. All individual employee assignments any daily work direction shall be given by the applicable employee supervisor.

(b) Hold him or herself out to be a Government employee, agent or representative or state orally or in writing at any time that he or she is acting on behalf of the Government. In all communications with third parties in connection with this contract, Contractor employees shall identify themselves as such and specify the name of the company of which they work.

(c) Be placed in a position of command, supervision, administration or control over Government personnel or personnel of other Government contractors, or become a part of the government organization. In all communications with other Government Contractors in connection with this contract, the Contractor employee shall state that they have no authority to change the contract in any way. If the other Contractor believes this communication to be direction to change their contract, they should notify the CO for that contract and not carry out the direction until a clarification has been issued by the CO.

4. If the Contractor believes any Government action or communication has been given that would create a personal service relationship between the Government and any Contractor employee, the Contractor shall promptly notify the CO of this communication or action.

5. Rules, regulations directives and requirements which are issued by U.S. Customs & Border Protection under their responsibility for good order, administration and security are applicable to all personnel who enter U.S. Customs & Border Protection installations or who travel on Government transportation. This is not to be construed or interpreted to establish any degree of Government control that is inconsistent with a non- personal services contract.

[End of Clause]

RIGHTS IN DATA-SBIR PROGRAM (MAY 2014)

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

"Computer database" or "database" means a collection of recorded information in a form capable of, and for the purpose of, being stored in, processed, and operated on by a computer. The term does not include computer software.

"Computer software"-

(1) Means.

(i) Computer programs that comprise a series of instructions, rules, routines, or statements, regardless of the media in which recorded, that allow or cause a computer to perform a specific operation or series of operations; and

(ii) Recorded information comprising source code listings, design details, algorithms, processes, flow charts, formulas, and related material that would enable the computer program to be produced, created, or compiled.

(2) Does not include computer databases or computer software documentation.

"Computer software documentation" means owner's manuals, user's manuals, installation instructions, operating instructions, and other similar items, regardless of storage medium, that explain the capabilities of the computer software or provide instructions for using the software.

"Data" means recorded information, regardless of form or the media on which it may be recorded. The term includes technical data and computer software. The term does not include information incidental to contract administration, such as financial, administrative, cost or pricing or management information.

"Form, fit, and function data" means data relating to items, components, or processes that are sufficient to enable physical and functional interchangeability, and data identifying source, size, configuration, mating and attachment characteristics, functional characteristics, and performance requirements. For computer software it means data identifying source, functional characteristics, and performance requirements but specifically excludes the source code, algorithms, processes, formulas, and flow charts of the software.

"Limited rights data" means data (other than computer software) developed at private expense that embody trade secrets or are commercial or financial and confidential or privileged.

"Restricted computer software" means computer software developed at private expense and that is a trade secret, is commercial or financial and confidential or privileged, or is copyrighted computer software, including minor modifications of the computer software.

"SBIR data" means data first produced by a Contractor that is a small business concern in performance of a small business innovation research contract issued under the authority of 15 U.S.C. 638, which data are not generally known, and which data without obligation as to its confidentiality have not been made available to others by the Contractor or are not already available to the Government.

"SBIR rights" means the rights in SBIR data set forth in the SBIR Rights Notice of paragraph (d) of this clause.

"Technical data" means recorded information (regardless of the form or method of the recording) of a scientific or technical nature (including computer databases and computer software documentation). This term does not include computer software or financial, administrative, cost or pricing, or management data or other information incidental to contract administration. The term includes recorded information of a scientific or technical nature that is included in computer databases. (See 41 U.S.C. 116.)

"Unlimited rights" means the right of the Government to use, disclose, reproduce, prepare derivative works, distribute copies to the public, and perform publicly and display publicly, in any manner and for any purpose whatsoever, and to have or permit others to do so.

(b) Allocation of rights.

(1) Except as provided in paragraph (c) of this clause regarding copyright, the Government shall have unlimited rights in-

(i) Data specifically identified in this contract as data to be delivered without restriction;

(ii) Form, fit, and function data delivered under this contract;

(iii) Data delivered under this contract (except for restricted computer software) that constitute manuals or instructional and training material for installation, operation, or routine maintenance and repair of items, components, or processes delivered or furnished for use under this contract; and

(iv) All other data delivered under this contract unless provided otherwise for SBIR data in accordance with paragraph (d) of this clause or for limited rights data or restricted computer software in accordance with paragraph (f) of this clause.

(2) The Contractor shall have the right to-

(i) Assert copyright in data first produced in the performance of this contract to the extent provided in paragraph (c)(1) of this clause;

(ii) Protect SBIR rights in SBIR data delivered under this contract in the manner and to the extent provided in paragraph (d) of this clause;

(iii) Substantiate use of, add, or correct SBIR rights or copyright notices and to take other appropriate action, in accordance with paragraph (e) of this clause; and

(iv) Withhold from delivery those data which are limited rights data or restricted computer software to the extent provided in paragraph (f) of this clause.

(c) Copyright-

(1) Data first produced in the performance of this contract.

(i) Except as otherwise specifically provided in this contract, the Contractor may assert copyright subsisting in any data first produced in the performance of this contract.

(ii) When asserting copyright, the Contractor shall affix the applicable copyright notice of 17 U.S.C. 401 or 402 and an acknowledgment of Government sponsorship (including contract number).

(iii) For data other than computer software, the Contractor grants to the Government, and others acting on its behalf, a paid-up nonexclusive, irrevocable, worldwide license to reproduce, prepare derivative works, distribute copies to the public, and perform publicly and display publicly, by or on behalf of the Government. For computer software, the Contractor grants to the Government, and others acting on its behalf, a paid-up, nonexclusive, irrevocable, worldwide license in such copyrighted computer software to reproduce, prepare derivative works, and perform publicly and display publicly, by or on behalf of the Government.

(2) *Data not first produced in the performance of this contract.* The Contractor shall not, without prior written permission of the Contracting Officer, incorporate in data delivered under this contract any data that are not first produced in the performance of this contract unless the Contractor (i) identifies such data and (ii) grants to the Government, or acquires on its behalf, a license of the same scope as set forth in paragraph (c)(1) of this clause.

(3) *Removal of copyright notices.* The Government will not remove any copyright notices placed on data pursuant to this paragraph (c), and will include such notices on all reproductions of the data.

(d) Rights to SBIR data.

(1) The Contractor is authorized to affix the following "SBIR Rights Notice" to SBIR data delivered under this contract and the Government will treat the data, subject to the provisions of paragraphs (e) and (f) of this clause, in accordance with the notice:

SBIR Rights Notice (Dec 2007)

These SBIR data are furnished with SBIR rights under Contract No. (and subcontract _____, if appropriate). For a period of 4 years, unless extended in accordance with FAR 27.409(h), after acceptance of all items to be delivered under this contract, the Government will use these data for Government purposes only, and they shall not be disclosed outside the Government (including disclosure for procurement purposes) during such period without permission of the Contractor, except that, subject to the foregoing use and disclosure prohibitions, these data may be disclosed for use by support Contractors. After the protection period, the Government has a paid-up license to use, and to authorize others to use on its behalf, these data for Government purposes, but is relieved of all disclosure prohibitions and assumes no liability for unauthorized use of these data by third parties. This notice shall be affixed to any reproductions of these data, in whole or in part.

(End of notice)

(2) The Government's sole obligation with respect to any SBIR data shall be as set forth in this paragraph (d).

(e) Omitted or incorrect markings.

(1) Data delivered to the Government without any notice authorized by paragraph (d) of this clause shall be deemed to have been furnished with unlimited rights. The Government assumes no liability for the disclosure, use, or reproduction of such data.

(2)If the unmarked data has not been disclosed without restriction outside the Government, the Contractor may request, within 6 months (or a longer time approved by the Contracting Officer in writing for good cause shown) after delivery of the data, permission to have authorized notices placed on the data at the Contractor's expense, and the Contracting Officer may agree to do so if the Contractor-

(i) Identifies the data to which the omitted notice is to be applied;

(ii) Demonstrates that the omission of the notice was inadvertent;

(iii) Establishes that the use of the proposed notice is authorized; and

(iv) Acknowledges that the Government has no liability with respect to the disclosure or use of any such data made prior to the addition of the notice or resulting from the omission of the notice.

(3)If the data has been marked with an incorrect notice, the Contracting Officer may-

(i) Permit correction of the notice at the Contractor's expense, if the Contractor identifies the data and demonstrates that the correct notice is authorized; or

(ii) Correct any incorrect notices.

(f) *Protection of limited rights data and restricted computer software.* The Contractor may withhold from delivery qualifying limited rights data and restricted computer software that are not identified in paragraphs (b)(1)(i), (ii), and (iii) of this clause. As a condition to this withholding, the Contractor shall identify the data being withheld, and furnish form, fit, and function data instead.

(g) *Subcontracting.* The Contractor shall obtain from its subcontractors all data and rights therein necessary to fulfill the Contractor's obligations to the Government under this contract. If a subcontractor refuses to accept terms affording the Government those rights, the Contractor shall promptly notify the Contracting Officer of the refusal and not proceed with the subcontract award without further authorization in writing from the Contracting Officer.

(h) *Relationship to patents.* Nothing contained in this clause shall imply a license to the Government under any patent or be construed as affecting the scope of any license or other right otherwise granted to the Government.

(End of clause)

I.13 POST AWARD EVALUATION OF CONTRACTOR PERFORMANCE (JUL 2014)

A. Contractor Performance Evaluations

Interim and final performance evaluation reports will be prepared on this contract or order in accordance with FAR Subpart 42.15. A final performance evaluation report will

be prepared at the time the work under this contract or order is completed. In addition to the final performance evaluation report, an interim performance evaluation report will be prepared annually to coincide with the anniversary date of the contract or order.

Interim and final performance evaluation reports will be provided to the contractor via the Contractor Performance Assessment Reporting System (CPARS) after completion of the evaluation. The CPARS Assessing Official Representatives (AORs) will provide input for interim and final contractor performance evaluations. The AORs may be Contracting Officer's Representatives (CORs), project managers, and/or contract specialists. The CPARS Assessing Officials (AOs) are the contracting officers (CO) or contract specialists (CS) who will sign the evaluation report and forward it to the contractor representative via CPARS for comments.

The contractor representative is responsible for reviewing and commenting on proposed ratings and remarks for all evaluations forwarded by the AO. After review, the contractor representative will return the evaluation to the AO via CPARS.

The contractor representative will be given up to fourteen (14) days to submit written comments or a rebuttal statement. Within the first seven (7) calendar days of the comment period, the contractor representative may request a meeting with the AO to discuss the evaluation report. The AO may complete the evaluation without the contractor representative's comments if none are provided within the fourteen (14) day comment period. Any disagreement between the AO/CO and the contractor representative regarding the performance evaluation report will be referred to the Reviewing Official (RO) within the division/branch the AO is assigned. Once the RO completes the review, the evaluation is considered complete and the decision is final.

Copies of the evaluations, contractor responses, and review comments, if any, will be retained as part of the contract file and may be used in future award decisions.

B. Designated Contractor Representative

The contractor must identify a primary representative for this contract and provide the full name, title, phone number, email address, and business address to the CO within 30 days after award.

C. Electronic Access to Contractor Performance Evaluations

The AO will request CPARS user access for the contractor by forwarding the contractor's primary and alternate representatives' information to the CPARS Focal Point (FP).

The FP is responsible for CPARS access authorizations for Government and contractor personnel. The FP will set up the user accounts and will create system access to CPARS.

The CPARS application will send an automatic notification to users when CPARS access is granted. In addition, contractor representatives will receive an automated email from CPARS when an evaluation report has been completed.
(End of Clause)

I.14 ADDITIONAL CONTRACTOR PERSONNEL REQUIREMENTS (OCT 2007)

The Contractor will ensure that its employees will identify themselves as employees of their respective company while working on U.S. Customs & Border Protection (CBP) contracts. For example, contractor personnel shall introduce themselves and sign attendance logs as employees of their respective companies, not as CBP employees.

The contractor will ensure that their personnel use the following format signature on all official e-mails generated by CBP computers:

[Name]
(Contractor)
[Position or Professional Title]
[Company Name]
Supporting the XXX Division/Office
U.S. Customs & Border Protection

[Phone]
[FAX]
[Other contact information as desired]

I.1 ENTERPRISE ARCHITECTURE COMPLIANCE

The Offeror shall ensure that the design conforms to the Department of Homeland Security (DHS) and Customs and Border Protection (CBP) Enterprise Architecture (EA), the DHS and CBP Technical Reference Models (TRM), and all DHS and CBP policies and guidelines (such as the CBP Information Technology Enterprise Principles and the DHS Service Oriented Architecture - Technical Framework), as promulgated by the DHS and CBP Chief Information Officers (CIO), Chief Technology Officers (CTO) and Chief Architects (CA).

The Offeror shall conform to the Federal Enterprise Architecture (FEA) model and the DHS and CBP versions of the FEA model, as described in their respective EAs. All models will be submitted using Business Process Modeling Notation (BPMN 1.1 or BPMN 2.0 when available) and the CBP Architectural Modeling Standards. Universal Modeling Language (UML2) may be used for infrastructure only. Data semantics shall be in conformance with the National Information Exchange Model (NIEM). Development solutions will also ensure compliance with the current version of the DHS and CBP target architectures.

Where possible, the Offeror shall use DHS/CBP approved products, standards, services, and profiles, as reflected by the hardware, software, application, and infrastructure components of the DHS/CBP TRM/standards profile. If new hardware, software, or infrastructure components are required

to develop, test, or implement the program, these products will be coordinated through the DHS and CBP formal Technology Insertion (TI) process (to include a trade study with no less than four alternatives, one of which reflecting the status quo and another reflecting multi-agency collaboration). The DHS/CBP TRM/standards profile will be updated as TIs are resolved.

All developed solutions shall be compliant with the Homeland Security (HLS) EA.

All IT hardware and software shall be compliant with the HLS EA.

Compliance with the HLS EA shall be derived from and aligned through the CBP EA.

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

Development of data assets, information exchanges, and data standards will comply with the DHS Data Management Policy MD 103-01. All data-related artifacts will be developed and validated according to DHS Data Management Architectural Guidelines.

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

(End of Clause)

[Name]
(Contractor)
[Position or Professional Title]
[Company Name]
Supporting the XXX Division/Office
U.S. Customs & Border Protection

[Phone]
[FAX]
[Other contact information as desired]

I.15 SPECIAL SECURITY REQUIREMENT - CONTRACTOR PRE-SCREENING (SEP 2011)

1. Contractors requiring recurring access to Government facilities or access to sensitive but unclassified information and/or logical access to Information Technology (IT) resources shall verify minimal fitness requirements for all persons/candidates designated for employment under any Department of Security (DHS) contract by pre-screening the person /candidate prior to submitting the name for consideration to work on the contract. Pre-screening the candidate ensures that minimum fitness requirements are considered and mitigates the burden of DHS having to conduct background investigations on objectionable candidates. The Contractor shall submit only those candidates that have not had a felony conviction within the past 36 months or illegal drug use within the past 12 months from the date of submission of their name as a candidate to perform work under this contract. Contractors are required to flow this requirement down to subcontractors. Pre-screening involves contractors and subcontractors reviewing:

    a. Felony convictions within the past 36 months. An acceptable means of obtaining information on felony convictions is from public records, free of charge, or from the National Crime Information Center (NCIC).
    b. Illegal drug use within the past 12 months. An acceptable means of obtaining information related to drug use is through employee self certification, by public records check; or if the contractor or subcontractor already has drug testing in place. There is no requirement for contractors and/or subcontractors to initiate a drug testing program if they do not have one already in place.

a. Misconduct such as criminal activity on the job relating to fraud or theft within the past 12 months. An acceptable means of obtaining information related to misconduct is through employee self certification, by public records check, or other reference checks conducted in the normal course of business.

2. Pre-screening shall be conducted within 15 business days after contract award. This requirement shall be placed in all subcontracts if the subcontractor requires routine physical access, access to sensitive but unclassified information, and/or logical access to IT resources. Failure to comply with the pre-screening requirement will result in the Contracting Officer taking the appropriate remedy.

Definition: *Logical Access* means providing an authorized user the ability to access one or more computer system resources such as a workstation, network, application, or database through automated tools. A logical access control system (LACS) requires validation of an individual identity through some mechanism such as a personal identification number (PIN), card, username and password, biometric, or other token. The

system has the capability to assign different access privileges to different persons depending on their roles and responsibilities in an organization.

3. Pre-screening shall be conducted within 15 business days after contract award. This requirement shall be placed in all subcontracts if the subcontractor requires routine physical access, access to sensitive but unclassified information, and/or logical access to IT resources. Failure to comply with the pre-screening requirement will result in the Contracting Officer taking the appropriate remedy.

Definition*:* *Logical Access* means providing an authorized user the ability to access one or more computer system resources such as a workstation, network, application, or database through automated tools. A logical access control system (LACS) requires validation of an individual identity through some mechanism such as a personal identification number (PIN), card, username and password, biometric, or other token. The system has the capability to assign different access privileges to different persons depending on their roles and responsibilities in an organization.

ISO Terms and Conditions for Sensitive but Unclassified Requests
DHS Security Policy Requirement
The following terms and conditions should be included in all acquisition documents.
All hardware, software, and services provided under this task order must be compliant with DHS 4300A DHS Sensitive System Handbook and the DHS Management Directive 140-01, Information Security Program.

Encryption Compliance Requirement
The following terms and conditions should be included in all acquisition documents.

1. *Systems requiring encryption shall comply with FIPS 197 (Advanced Encryption Standard (AES)) 256 algorithm and cryptographic modules that have been validated under FIPS 140-2.*
2. *Systems requiring encryption shall comply with National Security Agency (NSA) Type 2 or Type 1 encryption.*
3. *Only cryptographic modules that are FIPS 197 (AES 256) compliant and have received FIPS 140-2 validation at the level appropriate to their intended use may be used in systems requiring encryption.*

Public Key Infrastructure (PKI) (see paragraph 5.5.2.l of the Department of Homeland Security (DHS) Sensitive Systems Policy Directive 4300A.).
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. The Contractor shall provide access 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.

Interconnection Security Agreement (ISA)
The following requirements should be included in the acquisition document if the service being supplied requires a connection to a non-DHS, Contractor system, or DHS system of different sensitivity.
Interconnection Security Agreement Requirements
Interconnections between DHS and non-DHS systems shall be established only through the Trusted Internet Connection (TIC) and by approved service providers. The controlled interfaces are authorized at the highest security level of information on the network. Connections with other Federal agencies shall be documented based on interagency agreements, memorandums of understanding, Service Level Agreements (SLA) or Interconnection Security Agreements (ISA).

Required Protections for DHS Systems Hosted in Non-DHS Data Centers
The following requirements should be included in acquisition documents for information systems which are hosted, operated, maintained, and used on behalf of DHS at non-DHS facilities. Contractors are fully responsible and accountable for ensuring compliance with all Federal Information Security Management/Modernization Act (FISMA), National Institute of Standards and Technology (NIST) Federal Information Processing Standard (FIPS) and related DHS security control requirements (to include configuration guides, hardening guidance, DHS Security Policy, Procedures, and Architectural guidance). The contractor security procedures shall be equivalent to, if not more stringent than those that are provided by DHS Enterprise Data Center(s). Please note that all of the subsections from **Security Authorization** to **Log Retention** are included in this requirement.
All uses of cloud computing by DHS shall follow DHS security authorization processes and procedures to include developing a completed security authorization package and receiving an ATO signed by the appropriate Authorizing Official. Those cloud systems and services which are not exempt from FedRAMP requirements use the FedRAMP process as required by OMB.

Security Authorization
A Security Authorization of any infrastructure directly in support of the DHS information system shall be performed as a general support system (GSS) prior to DHS occupancy to characterize the network, identify threats, identify vulnerabilities, analyze existing and planned security controls, determine likelihood of threat, analyze impact, determine risk, recommend controls, perform remediation on identified deficiencies, and document the results. The Security Authorization shall be performed in accordance with the DHS Security Policy and the controls provided by the hosting provider shall be equal to or stronger than the FIPS 199 security categorization of the DHS information system.
At the beginning of the contract, and annually thereafter, the contractor shall provide the results of an independent assessment and verification of security controls. The

independent assessment and verification shall apply the same standards that DHS applies in the Security Authorization Process of its information systems. Any deficiencies noted during this assessment shall be provided to the COR for entry into the DHS' Plan of Action and Milestone (POA&M) Management Process. The contractor shall use the DHS' POA&M process to document planned remedial actions to address any deficiencies in information security policies, procedures, and practices, and the completion of those activities. Security deficiencies shall be corrected within the timeframes dictated by the DHS POA&M Management Process. Contractor procedures shall be subject to periodic, unannounced assessments by DHS officials. The physical aspects associated with contractor activities shall also be subject to such assessments. On a periodic basis, the DHS and its Components, including the DHS Office of Inspector General, may choose to evaluate any or all of the security controls implemented by the contractor under these requirements. Evaluation could include, but is not limited to, vulnerability scanning. The DHS and its Components reserve the right to conduct audits at their discretion. With ten working days' notice, at the request of the Government, the contractor shall fully cooperate and facilitate in a Government-sponsored security control assessment at each location wherein DHS information is processed or stored, or information systems are developed, operated, maintained, or used on behalf of DHS, including those initiated by the Office of the Inspector General. The government may conduct a security control assessment on shorter notice (to include unannounced assessments) determined by DHS in the event of a security incident.

Enterprise Security Architecture

The contractor shall utilize and adhere to the DHS Enterprise Security Architecture in accordance with applicable laws and DHS policies to the satisfaction of the DHS COR. Areas of consideration could include:

4. *Use of multi-tier design (separating web, application and data base) with policy enforcement between tiers*
5. *Compliance to DHS Identity Credential and Access Management (ICAM)*
6. *Security reporting to DHS central control points (i.e. the DHS Enterprise Security Operations Center (ESOC) and integration into DHS Security Incident Response*
7. *Integration into DHS Change Management (for example, the Infrastructure Change Control Board (ICCB) process)*
8. *Performance of activities per continuous monitoring requirements*

Continuous Monitoring

The contractor shall participate in DHS' Continuous Monitoring Strategy and methods or shall provide a Continuous Monitoring capability that the DHS determines acceptable. The DHS Chief Information Security Officer (CISO) issues annual updates to its Continuous Monitoring requirements via the Annual Information Security Performance Plan. At a minimum, the contractor shall implement the following processes:

9. *Asset Management*
10. *Vulnerability Management*
11. *Configuration Management*
12. *Malware Management*
13. *Log Integration*

14. Security Information Event Management (SIEM) Integration
15. Patch Management
16. *Providing near-real-time security status information to the DHS ESOC*

The Contractor shall establish a monitoring scope at least as comprehensive and stringent as described in DHS 4300A Sensitive Systems Handbook, Attachment F, "Incident Response."

Specific Protections

Specific protections that shall be provided by the contractor include, but are not limited to the following:

Security Operations

The Contractor shall operate a SOC to provide the security services described below. The Contractor shall support regular reviews with the DHS Information Security Office to coordinate and synchronize the security posture of the contractor hosting facility with that of the DHS Data Centers. The SOC personnel shall provide 24x7x365 staff to monitor the network and all of its devices. The contractor staff shall also analyze the information generated by the devices for security events, respond to real-time events, correlate security device events, and perform continuous monitoring. It is recommended that the contractor staff shall also maintain a trouble ticket system in which incidents and outages are recorded. In the event of an incident, the contractor facility SOC shall adhere to the incident response plan.

Computer Incident Response Services

The Contractor shall provide Computer Incident Response Team (CIRT) services. The contractor shall adhere to the standard Incident Reporting process as determined by the Component and is defined by a DHS-specific incident response plan that adheres to DHS policy and procedure for reporting incidents. The contractor shall conduct Incident Response Exercises to ensure all personnel are familiar with the plan. The contractor shall notify the DHS SOC of any incident in accordance with the Incident Response Plan and work with DHS throughout the incident duration.

Firewall Management and Monitoring

The Contractor shall provide firewall management services that include the design, configuration, implementation, maintenance, and operation of all firewalls within the hosted DHS infrastructure in accordance with DHS architecture and security policy. The contractor shall provide all maintenance to include configuration, patching, rule maintenance (add, modify, delete), and comply with DHS' configuration management / release management requirements when changes are required. Firewalls shall operate 24x7x365. Analysis of the firewall logs shall be reported to DHS COR in weekly status reports. If an abnormality or anomaly is identified, the contractor shall notify the appropriate DHS point of contact in accordance with the incident response plan.

Intrusion Detection Systems and Monitoring

The Contractor shall provide the design, configuration, implementation, and maintenance of the sensors and hardware that are required to support the Network Intrusion Detection System (NIDS) solution. The contractor is responsible for creating and maintaining the NIDS rule sets. The NIDS solution should provide real-time alerts. These alerts and other relevant information shall be located in a central repository. The NIDS shall operate 24x7x365. A summary of alerts shall be reported to the DHS COR in weekly status reports. If an abnormality or anomaly is identified, the contractor shall

notify the appropriate DHS point of contact in accordance with the incident response plan.

Physical and Information Security and Monitoring

The Contractor shall provide a facility using appropriate protective measures to provide for physical security. The facility will be located within the United States and its territories. The contractor shall maintain a process to control physical access to DHS IT assets. DHS IT Assets shall be monitored 24x7x365. A summary of unauthorized access attempts shall be reported to the appropriate DHS security office.

Vulnerability Assessments

The Contractor shall provide all information from any managed device to DHS, as requested, and shall assist, as needed, to perform periodic vulnerability assessments of the network, operating systems, and applications to identify vulnerabilities and propose mitigations. Vulnerability assessments shall be included as part of compliance with the continuous monitoring of the system.

Anti-malware (e.g., virus, spam)

The Contractor shall design, implement, monitor and manage a comprehensive anti-malware service. The contractor shall provide all maintenance for the system providing the anti-malware capabilities to include configuration, definition updates, and comply with DHS' configuration management / release management requirements when changes are required. A summary of alerts shall be reported to DHS COR in weekly status reports. If an abnormality or anomaly is identified, the contractor shall notify the appropriate DHS point of contact in accordance with the incident response plan.

Patch Management

The Contractor shall perform patch management services. The contractor shall push patches that are required by vendors and the DHS system owner. This is to ensure that the infrastructure and applications that directly support the DHS information system are current in their release and that all security patches are applied. The contractor shall be informed by DHS which patches are required by DHS through the Information Security Vulnerability Management bulletins and advisories. Core applications, the ones DHS utilizes to fulfill their mission, shall be tested by DHS. However, the contractor shall be responsible for deploying patches as directed by DHS. It is recommended that all other applications (host-based intrusion detection system (HIDS), network intrusion detection system (NIDS), Anti-malware, and Firewall) shall be tested by the contractor prior to deployment in a test environment.

Log Retention

Log files for all infrastructure devices, physical access, and anti-malware should be retained online for 180 days and offline for three years.

Product Assurance

Information Assurance (IA) is considered a requirement for all systems used to input, process, store, display, or transmit sensitive or national security information. IA is achieved through the acquisition and appropriate implementation of evaluated or validated commercial-off-the-shelf (COTS) IA and IA-enabled Information Technology (IT) products. These products provide for the availability of systems. The products also ensure the integrity and confidentiality of information and the authentication and nonrepudiation of parties in electronic transactions.

Strong preference is given to the acquisition of COTS IA and IA-enabled IT products (to be used on systems entering, processing, storing, displaying, or transmitting sensitive information) that have been evaluated and validated by authorized commercial laboratories or by NIST, as appropriate, in accordance with the following:
- The National Institute of Standards and Technology (NIST) FIPS validation program
- The NSA/NIST National Information Assurance Partnership (NIAP) Evaluation and Validation Program
- The International Common Criteria for Information Security Technology Evaluation Mutual Recognition Agreement

Supply Chain Risk Management Requirement

A supply chain threat is a man-made threat achieved through exploitation of the system's supply chain or acquisition process. A system's supply chain is composed of the organizations, people, activities, information, resources, and facilities for designing, creating and moving a product or service from suppliers through to the integrated system (including its sub-Components), and into service by the original acquirer.
Supply Chain risks result from adversarial exploitation of the organizations, people, activities, information, resources, or facilities that provide hardware, software, or services. These risks can result in a loss of confidentiality, integrity, or availability of information or information systems. A compromise to even minor system components can lead to adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.

Authorities:

- Comprehensive National Cybersecurity Initiative (CNCI) Initiative 11, Develop Multi-Pronged Approach for Global Supply Chain Risk Management
- Department of Homeland Security, Sensitive Systems Policy Directive 4300A
- Homeland Security Presidential Directive 23, Cyber Security and Monitoring, 8 January 2008
- Office of Budget and Management Circulation A-130, Appendix III
- •National Institute of Standards and Technology, Special Publication 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, April 2013

Supply Chain Risk Management

The following requirements should be included in all hardware and software requests to ensure the confidentiality, integrity, and availability of government information.

Contractors shall provide, implement, and maintain a Supply Chain Risk Management Plan that addresses internal and external practices and controls employed to minimize the risk posed by counterfeits and vulnerabilities in systems, components, and software. The Plan shall describe the processes and procedures that will be followed to ensure appropriate supply chain protection of information system resources developed, processed, or used under this contract. The Plan shall align with the Government's supply chain risk reduction strategy.
The Supply Chain Risk Management Plan shall address the following elements:

17. How risks from the supply chain will be identified,

18. *How commercial-off-the-shelf (COTS) hardware and software products considered for use in moderate and high criticality systems will be assessed for supply chain risk prior to acquisition, upgrade, or integration,*
19. *What processes and security measures will be adopted to manage these risks to the system or system components,*
20. *How the risks and associated security measures will be updated and monitored, and*
21. *How the Contractor will inform the Government of emerging risks, the status of managed risks, and risks becoming issues.*

The Supply Chain Risk Management Plan shall remain current through the life of the contract or period of performance. The Supply Chain Risk Management Plan shall be provided to the Contracting Officer's Representative (COR) 30 days post award. The Contractor shall review and update the Plan annually and following the identification of emerging risks requiring modification to the Plan. Updates to the Plan shall be provided to the COR within 30 days of the identification of the need for update.

The Contractor acknowledges the Government's requirement to assess the Contractors Supply Chain Risk posture. The Contractor understands and agrees that the Government retains the right to cancel or terminate the contract, if the Government determines that continuing the contract presents an unacceptable risk to national security.

The Contractor shall disclose, and the Government will consider, relevant industry standards certifications, recognitions and awards, and acknowledgments.

The Contractor shall provide only new equipment unless otherwise expressly approved, in writing, by the Contracting Officer (CO). Contractors shall only provide Original Equipment Manufacturers (OEM) parts to the Government. In the event that a shipped OEM part fails, all replacement parts must also be OEM parts.

The Contractor shall be excused from using new OEM (i.e. "grey market," previously used) components only with formal Government approval. Such components shall be procured from their original genuine source and have the components shipped only from manufacturers authorized shipment points.

For software products, the contractor shall provide all OEM software updates to correct defects for the duration of contract performance. Software updates and patches must be made available to the government for all products procured under this contract for the duration of performance.

Contractors shall employ formal and accountable transit, storage, and delivery procedures (i.e., the possession of the component is documented at all times from initial shipping point to final destination, and every transfer of the component from one custodian to another is fully documented and accountable) for all shipments to fulfill contract obligations with the Government.

All records pertaining to the transit, storage, and delivery will be maintained and available for inspection for the lesser of the term of the contract, the period of performance, or one calendar year from the date the activity occurred.

These records must be readily available for inspection by any agent designated by the U.S. Government as having the authority to examine them.

This transit process shall minimize the number of times en-route components undergo a change of custody and make use of tamper-proof or tamper-evident packaging for all

shipments. The supplier, at the Government's request, shall be able to provide shipping status at any time during transit.
The Contractor is fully liable for all damage, deterioration, or losses incurred during shipment and handling, unless the damage, deterioration, or loss is due to the Government. The Contractor shall provide a packing slip which shall accompany each container or package with the information identifying the contract number, the order number, a description of the hardware/software enclosed (Manufacturer name, model number, serial number), and the customer point of contact.

4.1.3.8 Personal Identification Verification (PIV) Credential Compliance

If the ITAR request is for products, systems, services, hardware, or software that enables access to controlled facilities and information systems, please include the PIV Credential Compliance requirement below.

Examples of when to use this requirement:

- The ITAR request is for a commercial-off-the-shelf (COTS) product that the Component requires to fulfill its mission requirements. The COTS product must be enabled to use PIV credentials, in accordance with NIST guidelines including Federal Information Processing Standard Publication (FIPS) 201 (Demonstrated progress toward integration with the DHS Application Authentication System (AppAuth) would be considered a confirmation to PIV enablement).
- The ITAR request is for the procurement of 1500 desktops as part of a technology refresh. The desktops must have a PIV card reader.
- The Component is requesting a custom software product to be developed. The custom software product must be able to use PIV credentials for authentication purposes.

Personal Identification Verification (PIV) Credential Compliance

Authorities:

- HSPD-12 "Policies for a Common Identification Standard for Federal Employees and Contractors"
- OMB M-11-11 "Continued Implementation of Homeland Security Presidential Directive (HSPD) 12– Policy for a Common Identification Standard for Federal Employees and Contractors"
- NIST FIPS 201 "Personal Identity Verification (PIV) of Federal Employees and Contractors"
- NIST SP 800-63-3 "Digital Identity Guidelines"
- NIST SP 800-63A "Digital Identity Guidelines: Enrollment and Identity Proofing"
- NIST SP 800-63B "Digital Identity Guidelines: Authentication and Lifecycle Management"
- NIST SP 800-63C "Digital Identity Guidelines: Federation and Assertions"
- OMB M-18-02 "Fiscal Year 2017-1018 Guidance on Federal Information and Privacy Security Management Requirements"

Personal Identification Verification (PIV) Credential Compliance Requirement

Procurements for products, systems, services, hardware, or software involving controlled facility or information system access shall be PIV-enabled by accepting HSPD-12 PIV credentials as a method of identity verification and authentication.
Procurements for software products or software development shall be compliant by accepting PIV credentials as the common means of authentication for access for federal employees and contractors.
PIV-enabled information systems must demonstrate that they can correctly work with PIV credentials by responding to the cryptographic challenge in the authentication protocol before granting access.
If a system is identified to be non-compliant with HSPD-12 for PIV credential enablement, a remediation plan for achieving HSPD-12 compliance shall be required for review, evaluation, and approval by the CISO.

CBP Contractor Handling PII Level

"When a contractor, on the behalf of CBP, handles Sensitive PII data, stores and transmits, the contractor will Accredit (ATO) this information system to the (HHM) FIPS level"

Security Requirements for Unclassified Information Technology Resources Requirement
If the contractor will be working on DHS sensitive data either at a contractor facility or on contractor equipment, a Contractor IT Security Plan is required. Insert a clause substantially the same as Homeland Security Acquisition Regulation (**HSAR) 3052.204-70** Security Requirements for Unclassified Information Technology Resources with the appropriate alternates.
Contractor Employee Access Clause
If the contractor requires recurring access to government facilities, or will require access to sensitive information, as prescribed in (HSAR) 48 CFR 3004.470-3(b), insert a clause substantially the same as **HSAR 3052.204-70, Security Requirements for Unclassified Information Technology Resources,** with appropriate alternates located in **HSAR 3052.204-71.**
The chart describes how to apply **HSAR 3052.204-71** to acquisition documents:

Task requires recurring access to Government facilities or access to sensitive information	Basic Clause (HSAR 3052.204-70)
Requires access to IT resources	Basic Clause + Alternate I
No IT access, but access to sensitive information is limited to U.S. Citizens & lawful permanent residents	Basic Clause + Alternate II (inapplicable)

As prescribed in (HSAR) 48 CFR 3004.470-3 Contract clauses, insert a clause substantially the same as follows:

Contracting officers shall insert a clause substantially the same as the clause at (HSAR) 48 CFR 3052.204-70, Security Requirements for Unclassified Information Technology Resources, in solicitations and contracts that require submission of an IT Security Plan.
(b) Contracting officers shall insert the basic clause at (HSAR) 48 CFR 3052.204-71, Contractor Employee Access, in solicitations and contracts when contractor employees require recurring access to Government facilities or access to sensitive information. Contracting officers shall insert the basic clause with its Alternate I for acquisitions requiring contractor access to IT resources. For acquisitions in which the contractor will not have access to IT resources, but the Department has determined contractor employee access to sensitive information or Government facilities must be limited to U.S. citizens and lawful permanent residents, the contracting officer shall insert the clause with its Alternate II. Neither the basic clause nor its alternates shall be used unless contractor employees will require recurring access to Government facilities or access to sensitive information. Neither the basic clause nor its alternates should ordinarily be used in contracts with educational institutions.

Basic Clause

3052.204-70 Security requirements for unclassified information technology resources.

SECURITY REQUIREMENTS FOR UNCLASSIFIED INFORMATION TECHNOLOGY RESOURCES (JUN 2006)

(a) The Contractor shall be responsible for Information Technology (IT) security for all systems connected to a DHS network or operated by the Contractor for DHS, regardless of location. This clause applies to all or any part of the contract that includes information technology resources or services for which the Contractor must have physical or electronic access to sensitive information contained in DHS unclassified systems that directly support the agency's mission.

(b) The Contractor shall provide, implement, and maintain an IT Security Plan. This plan shall describe the processes and procedures that will be followed to ensure appropriate security of IT resources that are developed, processed, or used under this contract.

(1) Within 60 days after contract award, the contractor shall submit for approval its IT Security Plan, which shall be consistent with and further detail the approach contained in the offeror's proposal. The plan, as approved by the Contracting Officer, shall be incorporated into the contract as a compliance document.

(2) The Contractor's IT Security Plan shall comply with Federal laws that include, but are not limited to, the Computer Security Act of 1987 (40 U.S.C. 1441 et seq.); the Government Information Security Reform Act of 2000; and the Federal Information Security Modernization Act of 2014; and with Federal policies and procedures that include, but are not limited to, OMB Circular A-130.

(3) The security plan shall specifically include instructions regarding handling and protecting sensitive information at the Contractor's site (including any information stored, processed, or transmitted using the Contractor's computer systems), and the secure management, operation, maintenance, programming, and system administration of computer systems, networks, and telecommunications systems.

(c) Examples of tasks that require security provisions include:

(1) Acquisition, transmission or analysis of data owned by DHS with significant replacement cost should the contractor's copy be corrupted; and
(2) Access to DHS networks or computers at a level beyond that granted the general public (e.g., such as bypassing a firewall).
(d) At the expiration of the contract, the contractor shall return all sensitive DHS information and IT resources provided to the contractor during the contract and certify that all non-public DHS information has been purged from any contractor-owned system. Components shall conduct reviews to ensure that the security requirements in the contract are implemented and enforced.
(e) Within 6 months after contract award, the contractor shall submit written proof of IT Security authorization to DHS for approval by the DHS Contracting Officer. Security authorization will proceed according to the criteria of the DHS Sensitive System Policy Directive, 4300A (Version 13.1, July 27, 2017) or any replacement publication, which the Contracting Officer will provide upon request. This accreditation will include a final security plan, security assessment plan, security assessment report, and contingency plan, and contingency plan test. This Authorization, when accepted by the Contracting Officer, shall be incorporated into the contract as a compliance document. The contractor shall comply with the approved Security Authorization documentation.
(End of clause)

3052.204-71 Contractor employee access.

As prescribed in (HSAR) 48 CFR 3004.470-3(b), insert a clause substantially the same as follows with appropriate alternates:

CONTRACTOR EMPLOYEE ACCESS (SEP 2012)

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

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

(2) Sensitive Security Information (SSI), as defined in Title 49, Code of Federal Regulations, part 1520, as amended, "Policies and Procedures of Safeguarding and

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

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

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

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

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

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

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

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

(End of clause)

Alternate I (SEP 2012) When the contract will require Contractor employees to have access to Information Technology (IT) resources, add the following paragraphs:

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

(h) The Contractor shall have access only to those areas of DHS information technology resources explicitly stated in this contract or approved by the 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 expressly authorized by the statement of work, other terms and conditions in this contract, or as approved in writing by the COR, is strictly prohibited. In the event of violation of this provision, DHS will take appropriate actions with regard to the contract and the individual(s) involved.

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

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

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

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

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

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

(End of clause)

SAFEGUARDING OF SENSITIVE INFORMATION (MAR 2015)

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(i) Security Authorization Process Documentation. SA documentation shall be developed using the Government provided Requirements Traceability Matrix and Government security documentation templates. SA documentation consists of the following: Security Plan, Contingency Plan, Contingency Plan Test Results, Configuration Management Plan, Security Assessment Plan, Security Assessment Report, and Authorization to Operate Letter. Additional documents that may be required include a Plan(s) of Action and Milestones and Interconnection Security Agreement(s). During the development of SA documentation, the Contractor shall submit a signed SA package, validated by an independent third party, to the COR for acceptance by the Headquarters or Component CIO, or designee, at least thirty (30) days prior to the date of operation of the IT system. The Government is the final authority on the compliance of the SA package and may limit the number of resubmissions of a modified SA package. Once the ATO has been accepted by the Headquarters or Component CIO, or designee, the Contracting Officer shall incorporate the ATO into the contract as a compliance document. The Government's acceptance of

the ATO does not alleviate the Contractor's responsibility to ensure the IT system controls are implemented and operating effectively.

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

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

(2) *Renewal of ATO.* Unless otherwise specified in the ATO letter, the ATO shall be renewed every three (3) years. The Contractor is required to update its SA package as part of the ATO renewal process. The Contractor shall update its SA package by one of the following methods: (1) Updating the SA documentation in the DHS automated information assurance tool for acceptance by the Headquarters or Component CIO, or designee, at least 90 days before the ATO expiration date for review and verification of security controls; or (2) Submitting an updated SA package directly to the COR for approval by the Headquarters or Component CIO, or designee, at least 90 days before the ATO expiration date for review and verification of security controls. The 90 day review process is independent of the system production date and therefore it is important that the Contractor build the review into project schedules. The reviews may include onsite visits that involve physical or logical inspection of the Contractor environment to ensure controls are in place.

(3) *Security Review.* The Government may elect to conduct random periodic reviews to ensure that the security requirements contained in this contract are being implemented and enforced. The Contractor shall afford DHS, the Office of the Inspector General, and other Government organizations access to the Contractor's facilities, installations, operations, documentation, databases and personnel used in the performance of this contract. The Contractor shall, through the Contracting Officer and COR, contact the Headquarters or Component CIO, or designee, to coordinate and participate in review and inspection activity by Government organizations external to the DHS. Access shall be provided, to the extent necessary as determined by the Government, for the Government to carry out a program of inspection, investigation, and audit to safeguard against threats and hazards to the integrity, availability and confidentiality of Government data or the function of computer systems used in performance of this contract and to preserve evidence of computer crime.

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

(5) *Revocation of ATO.* In the event of a sensitive information incident, the Government may suspend or revoke an existing ATO (either in part or in whole). If an ATO is suspended or revoked in accordance with this provision, the Contracting Officer may direct the Contractor to take additional security measures to secure sensitive information. These measures may include restricting access to sensitive information on the Contractor IT system under this contract. Restricting access may include disconnecting the system processing, storing, or transmitting the sensitive information from the Internet or other networks or applying additional security controls.

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

(f) *Sensitive Information Incident Reporting Requirements.*

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

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

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

(g) *Sensitive Information Incident Response Requirements.*

(1) All determinations related to sensitive information incidents, including response activities, notifications to affected individuals and/or Federal agencies, and related services (e.g., credit monitoring) will be made in writing by the Contracting Officer in consultation with the Headquarters or Component CIO and Headquarters or Component Privacy Officer.

(2) The Contractor shall provide full access and cooperation for all activities determined by the Government to be required to ensure an effective incident response, including providing all requested images, log files, and event information to facilitate rapid resolution of sensitive information incidents.

(3) Incident response activities determined to be required by the Government may include, but are not limited to, the following:

(i) Inspections,
(ii) Investigations,
(iii) Forensic reviews, and
(iv) Data analyses and processing.

(4) The Government, at its sole discretion, may obtain the assistance from other Federal agencies and/or third-party firms to aid in incident response activities.

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

(1) The Contractor shall have in place procedures and the capability to notify any individual whose PII resided in the Contractor IT system at the time of the sensitive information incident not later than 5 business days after being directed to notify individuals, unless otherwise approved by the Contracting Officer. The method and content of any notification by the Contractor shall be coordinated with, and subject to prior written approval by the Contracting Officer, in consultation with the Headquarters or Component Privacy Officer, utilizing the *DHS Privacy Incident Handling Guidance*. The Contractor shall not proceed with notification unless the Contracting Officer, in consultation with the Headquarters or Component Privacy Officer, has determined in writing that notification is appropriate.

(2) Subject to Government analysis of the incident and the terms of its instructions to the Contractor regarding any resulting notification, the notification method may consist of letters to affected individuals sent by first class mail, electronic means, or general public notice, as approved by the Government. Notification may require the Contractor's use of address verification and/or address location services. At a minimum, the notification shall include:

(i) A brief description of the incident;
(ii) A description of the types of PII and SPII involved;
(iii) A statement as to whether the PII or SPII was encrypted or protected by other means;
(iv) Steps individuals may take to protect themselves;
(v) What the Contractor and/or the Government are doing to investigate the incident, to mitigate the incident, and to protect against any future incidents; and
(vi) Information identifying who individuals may contact for additional information.

(i) *Credit Monitoring Requirements*. In the event that a sensitive information incident involves PII or SPII, the Contractor may be required to, as directed by the Contracting Officer:

(1) Provide notification to affected individuals as described above; and/or

(2) Provide credit monitoring services to individuals whose data was under the control of the Contractor or resided in the Contractor IT system at the time of the sensitive information incident for a period beginning the date of the incident and extending not less than 18 months from the date the individual is notified. Credit monitoring services shall be provided from a company with which the Contractor has no affiliation. At a minimum, credit monitoring services shall include:

(i) Triple credit bureau monitoring;
(ii) Daily customer service;
(iii) Alerts provided to the individual for changes and fraud; and
(iv) Assistance to the individual with enrollment in the services and the use of fraud alerts; and/or

(3) Establish a dedicated call center. Call center services shall include:

(i) A dedicated telephone number to contact customer service within a fixed period;
(ii) Information necessary for registrants/enrollees to access credit reports and credit scores;
(iii) Weekly reports on call center volume, issue escalation (i.e., those calls that cannot be handled by call center staff and must be resolved by call center management or DHS, as appropriate), and other key metrics;
(iv) Escalation of calls that cannot be handled by call center staff to call center management or DHS, as appropriate;

(v) Customized FAQs, approved in writing by the Contracting Officer in coordination with the Headquarters or Component Chief Privacy Officer; and
(vi) Information for registrants to contact customer service representatives and fraud resolution representatives for credit monitoring assistance.

(j) *Certification of Sanitization of Government and Government-Activity-Related Files and Information.* As part of contract closeout, the Contractor shall submit the certification to the COR and the Contracting Officer following the template provided in *NIST Special Publication 800-88 Guidelines for Media Sanitization.*

(End of clause)

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.

(End of clause)

STATEMENT OF WORK (SOW)

FOR THE
AUTONOMOUS SURVEILLANCE TOWERS (AST) SYSTEMS

DOCUMENT REVISION HISTORY

Version Number	Date	Description