DESCRIPTION/REQUIREMENTS/WORK STATEMENT
STATEMENT OF WORK (SOW)
FOR THE
AUTONOMOUS SURVEILLANCE TOWERS (AST) SYSTEMS
DELIVERY ORDERS 001 AND 002

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 (b) (7)(E) 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 (b) (7)(E) surveillance capabilities. Following the pilot an additional (b) (7)(E) were procured for deployment in (b) (7)(E) .

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, which 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) Autonomous Surveillance Towers (AST) Systems Delivery Orders 001 and 002. The AST shall be an (b) (7)(E) driven autonomous threat-detection capability that provides persistent, wide-area surveillance capabilities in operational environments along the southern, northern, and maritime borders.

The scope of this delivery order is to acquire, deploy, operate and sustain the autonomous surveillance capabilities necessary to fulfill operational requirements along the United States southern Borders. This contract allows for the procurement, sustainment, maintenance, test, deployment/re-deployment of this capability.

The contractor shall have total program responsibility for ensuring that the requirements in this SOW are met. The contractor shall provide program management, engineering, procurement, fabrication, manufacturing, installation, integration, testing, deployment/re-deployment, and sustainment for all CBP AST systems.

1. Order of Precedence

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

a. Contract requirements;

b. Capability Requirements; and

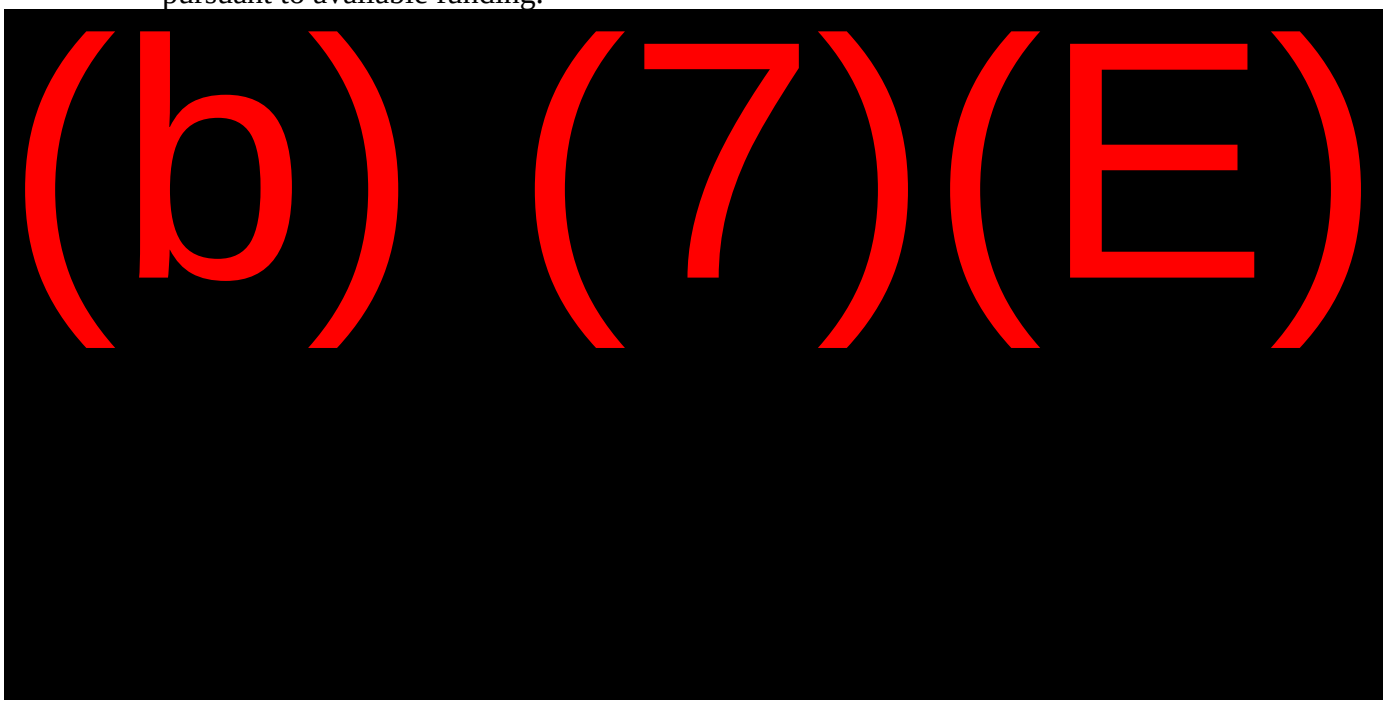
c. Government specifications and standards, industry standards, and similar referenced documents to include the DHS Acquisition Lifecycle Framework (ALF) and Systems Engineering Lifecycle (SELC)

C.3 GENERAL REQUIREMENTS

To meet CBP operational requirements, the contractor shall design, build, integrate, test, deliver/deploy, maintain, and sustain the AST in accordance with this SOW. Below is the high-level general requirements of delivery order 001 and delivery order 002.

Procurement (CLIN 001):

1) The contractor shall design, build, integrate, test, deliver/deploy, maintain, and sustain a total of (b) (7)(E) Towers in accordance with the SOW. Table 1 provides the anticipated deployment locations of the (b) (7)(E) systems. The Lattice Sentry MK IV systems shall include one (1) year of Operations & Support which begins from date of formal system acceptance by the government. The quantities on the delivery orders will be pursuant to available funding.



Note: Deployment plans are subject to future adjustments based on operational need.

2) The contractor shall design, build, integrate, test, deliver/deploy, maintain, and sustain (b) (4) AST Lattice Sentry Maritime Towers in accordance with the SOW. Table 2 provides the anticipated deployment locations of the three (3) AST Lattice Sentry Maritime Towers. The Lattice Sentry Maritime Towers shall include one (1) year of Operations & Support which begins from date of formal system acceptance by the government.

(b) (7)(E)

Operations & Sustainment (CLIN 002):

1) The contractor shall provide Operations & Sustainment for all currently deployed AST Lattice Sentry Towers. The contractor shall be solely responsible for sustaining the system to include all critical sensors during the contract period of performance. The contractor shall maintain all hardware and software components of the system in accordance with the requirements of the SOW. O&S shall start on all systems at the end of the existing contract sustainment support dates. Specific dates are denoted in the GFE Table in Section 16: GFE of the contract SOW. The contractor shall propose an approach to get all towers on the same contract sustainment schedule to terminate at the end of the delivery order period of performance.

(b) (7)(E)

2) The contractor shall provide Operations & Sustainment for all currently deployed (b) (7)(E) . The contractor shall be solely responsible for sustaining the system to include all critical sensors during the contract period of

performance. The contractor shall maintain all hardware and software components of the system in accordance with the requirements of the SOW. O&S shall start on all systems at the end of the existing contract sustainment support dates. Specific dates are denoted in the GFE Table in Section 16: GFE of the contract SOW. The contractor shall propose an approach to get all towers on the same contract sustainment schedule to terminate at the end of the delivery order period of performance.

(b) (7)(E)

2. Materials

The contractor shall provide a system specification for each system provided/sustained under this SOW (CDRL A001). The (b) (7)(E) is considered a family of systems that may be comprised of a combination of surveillance capabilities to include but not limited to modular relocatable towers and sensor heads, vehicle mounted, small emplaced sensors, and sUAS mounted/aerial sensor platforms.

The contractor shall ensure that all materials conform to the requirements specified in the AST systems Capability Requirement. The contractor shall be responsible for procuring and safeguarding the materials and components. To reduce costs and enhance equipment availability and support, the contractor shall utilize "commercial, off the shelf" equipment to the maximum extent possible.

At the end of the contract period of performance the system in the currently approved baseline to include all hardware, system and cloud software, system and technical data shall be transferred to the government for ownership, operation and sustainment (CDRL A002).

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 award (CDRL A002).

(a.) Shipping Address

Shipping addresses will be provided at time of award.

5. Program Management Plan and Monthly Reports

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

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 SELC documentation. 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 to the SELC may include, as reasonably applicable:

- Testing Artifacts (Acceptance Test Report and Operational Test and Evaluation)
- Systems Documentation Artifacts (Operator’s/User Manuals, Maintenance Manuals, Training Manuals
- Architecture Artifacts (Technology Insertion Design Request, Data Architecture Package, Data Service Insertion Package)

- Compliance Artifact Updates (Systems Security Plan, Security Risk Assessment, Contingency Plan, Contingency Test Plan, Security Test and Evaluation Plan, Interconnection Security Agreement, Security Assessment Plan and Report, Security Accreditation Plan, Security Authorization Updates).
- Privacy Artifact Updates (Privacy Documentation)
- Capital Planning and Investment Control (CPIC) – Operational Analysis
- Business Continuity Artifacts

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. Hardware

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 (b) (7)(E) 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. Operational availability requirements are defined in the capability requirements annexes. 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/GFE) List will be provided to the vendor at the time of award.

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 (CDRL A015). Detailed training requirements will be identified at time of award.

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. Recommended spare parts list;

C. List of special tools and test equipment; and

D. 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.

3. 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 (b) (7)(E) , within 30 days after ~~each delivery order is~~ award. 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 (b) (7)(E) 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. 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:

- (b) (7)(E)
- Metadata, Health & Status
- User & Group Logs/System Admin
- (b) (7)(E)
- Manual/Autonomous Control
- Usage Records
- Account Lists/Privileges
- (b) (7)(E) .

C.10 PERFORMANCE PERIOD

The period of performance for this effort begins upon the date of award for one-year.

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 [redacted] (b) (6), (b) (7)(C) [redacted]
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/
8	Code of Federal Regulations (CFR): http://www.gpoaccess.gov/cfr/index.html
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

Human image-labeling is critical to the computer vision component of the system to ensure consistent performance. The vendor is authorized to use images to train artificial intelligence (AI) algorithms in a manner consistent with the following requirements:

General Secure Supervised Learning (SSL) Requirements
All human image-labeling shall be conducted in a secure facility located in the United States.
Vendor shall ensure data remains in the United States.
The human image-labeling facility shall meet or exceed ISO 27001 or future equivalent as determined by CBP.
Vendor shall notify CBP within 24 hours of any identified security breach.
Vendor shall not use CBP data to train any model for any other customer or for any other purpose without CBP's prior written authorization.
Vendor will provide CBP with full security audit rights to the vendor physical/IT network that holds the CBP image data, sufficient to evaluate compliance with CBP requirements; CBP shall have full use of any of Vendor's audit rights applicable to third parties (see following section) and, if AWS is used for temporary storage of image data for labeling purposes, access to any AWS audit tools available to Vendor.
Vendor shall ensure that human faces in sample images are blurred and all other personally identifiable information (PII) is blurred and/or removed prior to human image-labeling activities. Vendor may store unblurred images in a CBP-approved system and used for training only with CBP authorization.
Vendor shall ensure that images are stripped of all metadata prior to human image-labeling, with the exception of metadata for (1) a Unique ID for the sensor system from which the data originated and (2) a time-stamp. Vendor may store additional image metadata separately in a CBP-approved system and may correlate this additional metadata back to labeled image data only with CBP authorization.
Image samples used for labeling shall in no way possess metadata, labeling, etc. that identifies the image as CBP data. Any information (including metadata) that could be used to identify image samples as CBP data must be stored separately from image samples in a secure, CBP-approved system and only correlated with image samples for training purposes with CBP authorization.
All image samples shall be (b) (7)(E) [redacted] in transit and at rest.
Vendor shall obtain CBP authorization prior to sharing image samples with any third party.
Vendor shall store labeled images and access the labeled images only for the purpose of training models.
Vendor is authorized to store labeled images for the duration of contract period of performance, unless directed otherwise by CBP. Vendor shall destroy labeled images upon CBP direction or at the conclusion of the contract period of performance.

CBP authorizes the vendor to contract a human image-labeling service that meets or exceeds the requirements stated above as well as the following additional requirements:

Third Party Secure Supervised Learning (SSL) Requirements
CBP shall have the ability to review the contractual agreement between Vendor and any third party human image-labeling service, to ensure that all CBP security and privacy protection requirements are met.
The third party shall be subject to strict contractual prohibitions on data misuse, reuse, repurposing, or security violations.
The third party human image-labeling service shall be under NDA with the vendor and put each labeler under individualized NDA.
CBP shall have the ability to confirm the existence of properly-executed non-disclosure agreements upon request.
The third party shall be contractually obligated to conduct background-checks on human labelers.
Vendor shall provide CBP a roster of authorized labelers upon request.
Image samples shall be available to third party human image-labelers for no longer than the period of time required to label the data.
Vendor shall institute appropriate controls (ex. tokenization) to ensure that the third party access to the data is invalidated upon completion of the labeling task.
Vendor shall not disclose the source of the image samples (i.e., CBP), the end-user (i.e., CBP), or the application of the AI model to any third party human image-labeling service personnel or representative.