Air Carrier Analysis Support System (ACAS) Application & System Support Performance Work Statement (PWS)

Name:	**AIR CARRIER ANALYSIS SUPPORT SYSTEM (ACAS) APPLICATION & SYSTEM SUPPORT**
Organization:	**AIR MOBILITY COMMAND (AMC) DIRECTORATE OF OPERATIONS (HQ AMC/A3BA)**
Address:	**402 Scott Drive, Scott AFB, IL 62225**

Executive Summary

Title 10 U.S. Code Section 2640 and Department of Defense (DOD) Instruction 4500.53 mandates that the DOD evaluate operations, maintenance, and safety programs of any commercial air carriers providing or seeking to provide airlift services to the DOD. AMC A3B has been charged with the responsibility of performing the safety oversight of commercial air carriers participating in the DOD Air Transportation Program and the management of the Civil Reserve Air Fleet (CRAF). These mission partners in the commercial industry are responsible for moving ~93% of our DOD personnel and over 40% of our cargo each year. Operational decision making is essential to the Commercial Airlift Division processes and business. The capability to provide fact-based decision making and aggregate appropriate data is done in the ACAS.

Air Carrier Analysis Support System (ACAS) Application & System Support PWS

PURPOSE

ACAS is a web-based application for HQ AMC/A3B and USTRANSCOM AQ communities to support the safety oversight of commercial air carriers currently engaged or desiring business with the DOD. ACAS is essential to providing an integrated operational capability for safety analysis of accidents and incidents, operations, maintenance, financial analysis, and service quality information for both domestic and foreign commercial air carriers supporting DOD. ACAS provides every user the ability to pick from numerous capabilities within the system such as scheduling, CRAF, queries, data collection, and reports. Integrated within those focused areas are detailed information from the Federal Aviation Administration (FAA), National Transportation Safety Board (NTSB), USTRANSCOM Contract Airlift Division (TCAQ), news reports and others that populate data on every airline to accommodate fact-based decision making in a timely manner.

Furthermore, ACAS is utilized in supporting the management of the CRAF, tracking aircraft data, analysis of wartime civilian airlift capacity, and assignment of civilian aircraft to wartime stages. The ability to aggregate this data is critical to the Commercial Airlift Review Board (CARB) that is a General Officer/Flag Officer appointed panel by United States Transportation Command (USTRANSCOM) Commander (TCCC) for direct oversight and timely management decisions for DOD on safety issues. ACAS integrates commercial air carrier information from multiple Government agencies/systems and commercial sources to include the DOD, FAA, and NTSB. Centralizing information into a single system drastically improves the efficiency and capability of safety oversight by providing analysis of disjointed data. ACAS operates at Scott AFB, with an alternate site at McConnell AFB, and supports users at HQ AMC, USTRANSCOM, and HQ FAA. In addition, there are a number of electronic data exchange with other AMC and USTRANSCOM systems, and external organizations such as the FAA and the Defense Transportation Management Organization (DTMO). For the FAA system expertise and mission partnership AMC relies on the Department of Transportation, Volpe National Transportation System Center. An understanding of the processes for the sustainment and maintenance of ACAS is important. At the highest level, the A3 Government team supports the activities for ACAS with technical expertise from our Program Manager (PM) and Systems Manager (GSM) and the operational expertise of our Functional Manager (GFM). This is the expertise of the ACAS Government team. The PM, GSM and GFM are responsible for management and oversight of the ACAS program while ensuring the operational system meets the needs of senior leaders and ACAS users and maintaining compliance with DOD directives and local policy or standards.

OBJECTIVE

The objective of this requirement is to (1) update existing system software and sustainment support, (2) migrate ACAS into the USTRANSCOM cloud environment, (3) provide operations and maintenance support, and (4) cybersecurity support for ACAS. This includes all software code and associated components and integrations. Software development support shall include all phases of the Software Development Lifecycle (SDLC), including concept development, planning, requirements elicitation and analysis, systems design and development, coding and testing, deployment, implementation, integration, troubleshooting, security posture, documentation, and software application maintenance.

Responsibilities include managing the code baseline, the hosted environments, and system interfaces. The code baseline may change as a result of user preference, latent defects, change requests, security requirements, or updates to Commercial Off The Shelf (COTS) products use by the system. Additionally, the Contractor shall provide production support to include troubleshooting and resolving user problems as well as identifying opportunities to improve the system. Overall, software development support shall include all aspects of the SDLC necessary to sustain and modify the system baseline. The Contractor shall work closely with other members of the team to include Government Program Manager (PM), Program Management Office (PMO), Product Owners (PO), engineers, security, and end-users. PM and PMO can act, in their own capacity as a collective authority Functional Manager (FM) also can act on the behalf of the Government regarding functional capabilities and requirements within ACAS. The PMO is a collection of system management roles, including PM, Lead Government Engineer, Government Program Office Lead, and System Manager.

SCOPE

The Contractor shall provide agile software baseline modernization and sustainment support for ACAS. The Contractor shall provide solution consulting and programming to: (1) implement new system capabilities; (2) implement change requests; (3) sustain deployed capabilities by rapidly troubleshooting and repairing software issues (i.e. correct software defects); (4) provide technical expertise to ensure high availability of the application to meet the AMC and USTRANSCOM mission; (5) receive and respond to problems reported by system users (i.e. correct incidents); (6) improve the system's security posture. The Contractor shall provide expert support in achieving the discipline of Development/Security/Operations (DevSecOps) and Continuous Integration/Continuous Delivery (CI/CD).

Further, the Contractor shall provide expertise to build and maintain the ACAS development, non-production, and production environments in the forthcoming Cloud Computing Environment (CCE) provided by TRANSCOM using infrastructure as code principles. The Contractor shall migrate ACAS from its on-site hosting environment to the CCE. The Contractor shall implement DevSecOps strategies and develop and maintain an automated CI/CD pipeline to promote ACAS from development to non-production and productions environments in the CCE. The Contractor shall provide operation and maintenance support of the development, non-production, and production environments in the CCE, to include help desk support.

The Contractor shall provide all qualified personnel, equipment, and materials (not to include Government furnished equipment and property spelled out in this document) required to execute the work defined in this PWS and offered within the contractor's accepted proposal.

The Contractor shall provide qualified personnel with relevant experience and domain knowledge in line with this task's performance work statement, in terms of necessary skills at the requisite level of knowledge and experience. Broadly, a team assigned to build and sustain ACAS is expected to be highly qualified and have extensive demonstrated experience with building and testing web-based applications, user-centered design practices, Agile and scrum methodologies, DevSecOps and automated CI/CD pipelines, cloud architecture, cloud deployment, system security engineering, Risk Management Framework, usability testing, automated testing, user experience and visual design, Java, JSP, PL/SQL, microservices, open-source login / authentication services, data modeling, RHEL, Oracle database, Apache Tomcat, Apache HTTP Server etc.

The specific performance activities and deliverables associated with the technical requirements are captured below:

1. Task Area 1: Contract Level Task and Program Management

This task includes, but not limited to the activities related to the administration and management of this effort. The Contractor shall provide the planning, direction, coordination, and control necessary to accomplish all requirements in this PWS. The Contractor shall designate key personnel responsible for the performance for the contract and shall serve as a primary Point of Contact (POC) for both management and technical matters. The Contractor shall provide program management for all Contractor tasks, personnel resources and ensure all deliverables meet requirements for acceptance under this PWS. The Contractor shall provide personnel who meet the technical and experience requirements to fulfill requirements of the PWS. In addition, the Contractor shall participate in Program Management Reviews where the status of the work and associated deliverables are reviewed in the context of the business processes supported by the system.

1.1. Program Management

The Contractor shall:

- Provide an individual capable of fulfilling the Program Manager (PM) position responsible for the performance of the work. The name of the PM and alternate(s), who shall act for the Contractor when the PM is absent, shall be designated in writing to the Contracting Officer (CO) at contract award and when personnel changes occur.
- Ensure all personnel assigned to this contract meet the minimum requirements specified in the Contractor's staffing approach proposal and this PWS.
- Provide a Management Plan (MP) to document the Contractor's approach executing the tasks defined in the PWS. The contractor shall provide a draft MP with the proposal submission. The MP shall describe management's plan to track the quality/timeliness of deliverables, organizational resources, and management controls to be employed to meet performance requirements.
- Implement a risk management program, documenting the Risk Management approach in the MP.
- Provide personnel with expertise in the subject matter areas to comply with the terms of this PWS. The Contractor personnel shall be capable of working independently and with demonstrated knowledge as described in the terms of this PWS.
- Ensure personnel remain current in all requirements and certifications required to perform duties specified in this contract and applicable statutory and regulatory requirements. Provide a Monthly Status Report (MSR).
- Document risk identification and assessment and summarize open risks in the MSR.
- Include an Employment Status Report (ESR) section as part of the MSR. The Employment Status section shall contain names, positions, and labor categories of personnel supporting each task. The initial ESR report shall be provided within twenty (20) business days after performance start and shall be consistent with the Contractor's accepted proposal. Changes in staffing from the initial proposal's staffing plan or as the result of subsequent modifications to

the contract shall be identified and rational for the change provided to the Government. Subsequent reports shall be delivered within five (5) business days after changes in key personnel.

- Provide and maintain a product roadmap (a strategic overview) to plan out new system capabilities, functionality changes, system maintenance, and/or product upgrades. The product roadmap shall include, at a minimum the current release, release+1, and release+2. The product roadmap shall be updated after each iteration. The Contractor shall collaborate with the Contract Officer's Representative (COR) to obtain the Government's priority on software features and product updates.

1.2. Program Reviews and Technical Exchange Meetings

The Contractor shall:

- Meet with the PO/PM/PMO and/or designated Government personnel weekly to review status of work in progress, discuss problems with current tasks and assignment of future tasks, and get Government decisions or guidance necessary to facilitate or improve Contractor performance
- Deliver agenda, minutes, and presentation slides for all meetings the Contractor facilitates/leads or as required by the Government. At a minimum, the minutes shall reflect date, location, attendees, a record of current and planned activities, decisions made, and action items.
- The Contractor shall schedule, facilitate and participate in technical exchange meetings (TEM) with the Mission Partners or other interested parties. The focus of the meetings will be to convey technical/functional information regarding the capabilities, discuss identified issues with the existing operational baseline, or gather information to support enhancements/develop of new capabilities. The Contractor shall prepare agendas, presentation slides to aid discussions and minutes.
- Meet with the ACAS PM and ACAS partners monthly to exchange information. The contractor shall prepare presentations and brief schedule status, risks, issues, and progress of each assigned task, plus any other topic identified by the ACAS PM. This participation will involve work with other contractors, Government, and Federally Funded Research and Development Center (FFRDC).

1.3. Program Reporting

The Contractor shall provide ~~an~~ input to the Government's higher level program reviews or portfolio briefings, as needed.

1.4. Monthly Status Report (MSR)

The Contractor shall provide a Monthly Status Report (MSR).

The report shall include:

- all task- related activities accomplished in the past month
- projected significant activities for the upcoming month
- open issues requiring Government resolution

- open risks and adjustments to the Integrated Master Schedule ~~IMS~~
- summary of the problem management Help Desk activities to include
    - support provided to end users
    - tickets received and closed
    - status of open tickets
    - number/type of incidents
    - average time to resolve
    - age of unresolved incidents
    - any trends identifying common user/technical problems
    - significant sustainment actions and recommendations for improvement and Help Desk metrics
- employment status section shall include
    - names
    - positions
    - labor categories of personnel supporting each task.
    - changes in staffing from the initial proposal's staffing plan or as the result of subsequent modifications to the contract shall be identified and rational for the change provided to the Government.

1.5. Software Development and Maintenance Integrated Master Schedule

The Contractor shall create and maintain and provide an Integrated Master Schedule (IMS) containing the performance and schedule requirements including requirements analysis, coding, testing, and delivery throughout contract execution using MS Project or other government approved project scheduling software tool.

1.6. Technical Reporting

The Contractor shall develop and provide Technical Reports based on Government requests or Contractor initiatives upon approval from the Government. The Contractor shall include the following information in the Technical Reports:

- Identify and recommend courses of action/changes and/or technology upgrades to address performance and cybersecurity issues, standardization, and industry best practices
- Provide concept definition, technology evaluation, rationale and planning support for technology transition
- Rough order of magnitude and labor categories needed to complete the action
- Risk analysis

2. Task Area 2 - Configuration Management (CM) and Quality Assurance (QA) Support

The Contractor shall perform CM and QA tasks which includes, but not limited to configuration management (CM) and quality assurance (QA) to assist the program in meeting AMC and USTRANSCOM technical and cybersecurity requirements. The CM system is used to keep track of an organization's software, and related information. This includes software versions and updates installed

on the organization's computer systems along with documentation associated with the software versions, updates and builds. CM also involves logging network addresses belonging to systems.

The CM and QA processes facilitate orderly configuration identification, change identification and control, status reporting and auditing of product information. CM ensures that changes take place in an identifiable and controlled process and do not adversely affect the properties of other system or interfaces. QA establishes and maintains the integrity of the products of a project throughout the project life cycle. CM involves identifying the configuration items of products developed and delivered to the customer, systematically controlling changes to the configuration, and maintaining configuration traceability.

The Contractor shall develop an internal Configuration Management Plan (CMP), Quality Program Plan (QPP) and processes that are consistent with the Government CMP.

The contractor shall establish and maintain a QPP in accordance with ISO/IEC 26514:2008 and Software Engineering Institute (SEI) Capability Maturity Model - Integrated (CMMI) Level 3-Defined requirements. In establishing and maintaining a QPP, the contractor shall plan, develop, and implement procedures and practices to ensure that all requirements of the contract are complied with fully. The government representative shall audit all processes and products as outlined in the QPP. The QPP shall also include a non-compliance reporting and tracking process.

The contractor shall support government reviews and audits of all services and support provided under this contract. The government reserves the right to authorize an independent verification and validation of the contractor's procedures, methods, data, equipment, and other services provided at any time during the performance of this contract. At government's discretion, registered ANSI/ISO/ANSQ Q9000 series suppliers may not be subjected to audit/assessment by government if they provide the government with a copy of their registration certification issued by an approved ISO registrar.

Using MIL HDBK 61A, ISO/IEC/IEEE 12207:2017, and EIA 649 guidance, the contractor shall institute and maintain a configuration management process to ensure engineering and administrative disciplines (which include configuration identification, configuration control, status accounting, and auditing) are implemented for all development activities. The contractor shall identify the configuration of all work products (to mean baselines as well as other supporting work products), systematically control changes, and maintain the integrity and traceability of all work products throughout their lifecycle. The contractor shall ensure configuration is identified, reliable, traceable, and repeatable, and that all relationships among work products, versions of work products, as well as auditing and reporting on the changes that are made are implemented throughout the development process.

The Contractor shall administer and maintain baseline configurations based on the agreed upon builds. This includes providing management of changes and status to all Configuration Item(s) (CIs) including software components, sustainment builds, related documentation, and disposition status of change requests.

The Contractor shall provide change control for all baselines and configuration items to include documentation, hardware, COTS software, application, source, and executable code. The System of Record shall employ their change control process to identify, track, and develop all changes attributable to CRs and other changes made in support of the program. The Government will provide web access to

the Change Request System and to the trouble ticketing system for the Contractor's Help Desk and sustainment personnel.

The Government requires the Contractor to utilize an Agile software development and DevSecOps methodologies to enhance existing and deliver new capabilities. The Government will provide the Contractor access to an Agile Management Tool (AMT) to assist the Contractor in managing and tracking use cases, user stories, tasks, exit criteria and other related information that can be traced back to a change request. The SDP shall document the Contractor's implementation of Agile Scrum.

3. Task Area 3: Software Development Support

This task includes responding to requirements that are generated by the Government through change requests, program, security, production support, or trouble reporting mechanisms. This task also includes responding to Application Lifecycle Management (ALM) artifacts (i.e. new requirements) to implement new capabilities in the system (i.e. different than implementing change requests to existing capabilities). New capabilities will focus on creating new/additional system operational activities. ALM artifacts are the method for identifying software changes and new capabilities, which will be deployed into the Production environment. This task shall include all Agile Software Development Life Cycle (SDLC) activities to support implementing software changes and new capabilities. The Contractor shall properly record user stories, associated acceptance criteria, issues, and software solutions to create a knowledge base within the Government's ALM tool. The Contractor shall use the Agile Scrum Framework; along with microservices architecture and extreme programming engineering practices such as test-driven development, refactoring, and continuous integration; when completing artifacts to include: requirements elicitation and decomposition, completion of user stories and specifications, software development, security code scans, unit testing, integration testing, and User Acceptance Testing (UAT). The Contractor shall use a microservices architecture for new code, and decouple monolithic legacy code when appropriate (e.g. failure isolation, multiple rates of change, simplify external dependencies, etc.) for long-term usability and scalability of the application. Additionally, the Contractor shall automate testing, security updates, configuration management, the software build and deployment processes, etc. necessary to achieve an automated DevSecOps and CI/CD pipelines.

In accomplishing this task the contractor shall provide

- Software. The primary deliverable of this task is software code, system configurations, database schemas, etc. resulting from this task. All software code, system configurations, database schemas, etc. associated with this contract shall be the property of the Government and shall not contain any company proprietary markings, logos, or any distribution restrictions. Software code shall be installed on the Government's Staging and Production servers and provided as a tagged code segment via the Government managed code repository and/or delivered on other mutually agreed upon format
- Release Documentation. As a minimum, this shall include a work plan with recurring updates, static code scans (e.g. Fortify scans), release test plan with results, UAT plan with test scripts, and minor mod checklists (i.e. release notes), which include all artifacts with associated descriptions and solutions, and deployment instructions. Release documentation includes, Logical Data Model, Physical Data Model, System/Subsystem Design Description, Software Requirement Specification, Interface Requirement Specification, Software Test Plan, Software Test Description, Software Test Reports, Operations

- Updated Project Documents. Documentation sufficient to install, operate, and maintain the system shall be provided and maintained. These documents shall include updates to the product roadmap, COTS products, training manuals, user manuals, system installation procedures, and any supporting documents necessary for the Government to sustain the system. Documentation includes Operations Manual, Software Installation Instructions, Software User Manual.
- Updated System Documents, Security Documents, White Papers. All solution changes shall be documented as user stories, technical specifications and/or diagrams, interface control documents, system configuration documents, and/or Department of Defense Architecture Framework (DODAF) architectural artifacts. Additionally, documentation will be generated and maintained to support Static Code Analysis, the Risk Management Framework (RMF), Defense Information Systems Agency (DISA) DISA Security Technical Implementation Guides (STIGs), DISA Security Requirements Guides (SRGs), DODI 8530.01, DOD 8570.01-M (Information Assurance Workforce Improvement Program), and the DOD Cloud Computing Security Requirements Guide. Security documents as a minimum shall include STIG Checklists, Ports Protocols & Service Matrix, Logical Network Topology Diagram.

3.1. Agile Software Development and Sustainment Support

The Contractor shall respond to ALM artifacts to change the system, as prioritized and assigned by the Government PO/PM. The Contractor shall lead and participate in the Scrum process and other meetings to define, build, test, document, and deploy updates to the system baseline, with activity defined in the Software Development Plan. The Contractor shall ensure ample lead-time for understanding and responding to unique change requests. The planning for requested functionality may include the Contractor's recommendations to minimize rework and cost. If a change is beyond the Contractor's capacity to complete within one sprint, the Contractor shall decompose the Epic and/or features into smaller user stories; and update the schedule (i.e. product roadmap). Complex tasks may require additional planning before coding. These tasks are assigned to a sprint for development of a specification prior to the implementation sprint. The Contractor shall work with subject matter experts to create, and receive approval on, user stories and associated acceptance criteria, functional specifications and/or technical specifications. The definition of done is when Government accepts a release/fix and is determined ready for fielding into the Operational Environment. The Contractor shall support UAT for releases to ensure proposed changes are acceptable to users; and, when required, host release reviews for functional users to illustrate system changes. The Contractor shall assist with minor modification checklists (i.e. release notes); and shall provide necessary support to maintain and document the security posture of the application as required by the RMF or applicable DOD accreditation process.

3.2. Product Road Map and Backlog

The Contractor, in coordination with the PO/PM, shall document, manage, and maintain the product roadmap. The items identified in the roadmap shall align to the overall product vision and be organized by capabilities/features. The Contractor, in coordination with the Product Owner, shall use the roadmap to organize and populate the Backlog, prioritize work, and ensure that the appropriate capabilities/features are being delivered at the right time. The contractor shall adjust the product roadmap and backlog, in consultation with the PO/PM prior to each release/sprint planning event.

The contractor shall provide the PM/FM/PO with an estimate of the effort required to develop each item in the Product Backlog, based on Government priority and roadmap. These estimates shall be prepared with appropriate care and skill and on the basis of fair and reasonable assumptions.

The contract shall normalize story point estimation so that estimates for features or epics are based on the same story point definition, allowing a shared basis for decision-making. The contractor shall use the following to normalize story point estimation: one story point takes about a day to develop and test; that is, about a half-day to develop and a half-day to test and validate. No refinement hours shall be included in the point value.

Once the contractor estimates of effort are finalized, the PM/FM will assign a priority to each functional item based on the estimates of effort and business value. PM will prioritize each non-functional item, as needed.

It should be understood, the FM/PM is free to amend the Product Backlog, as needed, with review by FM and coordination with PM. However, the PO cannot unilaterally change the estimates of effort received from the Contractor, although they can be disputed; and the scope or priority of items cannot be changed once they are under development as part of a Sprint.

In collaboration with the PO/PM, the Contractor shall provide stories with the requisite information. A story represents any unit of measurable work that provides value to the Government and shall serve as the basis for measurable work/deliverables.

Stories shall include the following information and entered into the Enterprise Platform (e.g., Jira):
1) Title
2) Description
3) Level of Effort (e.g., story points)
4) Business Value
5) Definition of Done
6) Acceptance Criteria
7) Dependencies
8) Other attributes that characterize the story

Stories shall fall into one of four states:
a) Proposed: The story is complete (contains the required attributes) but has not been approved by the PO/PM.
b) Approved: The story has been approved and work can begin.
c) In-Progress: The story is approved, assigned to a team, and is currently under development.
d) Done: The story has been completed (meeting the definition of done and all acceptance criteria) and is accepted by the Government.

Prior to executing any work, the Contractor shall develop (in conjunction with stakeholders) a user story and obtain approval. It is assumed the creation of stories may require participation from multiple stakeholders, to include SMEs, PO, Functional Manager, and Program Manager. The Contractor shall be responsible for coordinating all activities required to complete each story. The Contractor shall be responsible for tracking and decomposing each story down to the working level

(generally requiring less than 10 business days to complete the story). The Contractor shall clearly show traceability and dependencies between stories. The Contractor shall develop milestones and a detailed schedule for more complex stories.

The Contractor shall collaborate with the Government representative and other subject matter experts to review and document the Minimum Viable Product (MVP). The contractor shall ensure the MVP description identifies the features that provide just enough capability to the end-users to enable them to provide feedback to influence future development sprints.

The Contractor shall, in consultation with the PM/PMO and facilitated by the Contractor's Scrum Master, allocate backlog items to Sprints that align to the roadmap. The Contractor shall deliver the MVP within the allotted timeframe. End-user feedback shall be documented and reviewed with the PO/PM.

The Contractor shall work closely with the PM/PO/FM, to ensure the Product Backlog is continually and regularly maintained in alignment with the Agile cadence so that the necessary Release and Sprint Backlog items (epics, features, and user stories) are defined with acceptance criteria and prioritized by the PM/PO/FM-on a continual basis, so backlog is ready for each release and sprint. The Contractor will ensure backlog items are defined well enough for development/programming efforts, and requirement is understood well enough to be delivered as planned and meets originator's needs. The Contractor shall sequence backlog items to ensure release/sprint planning does not produce blockers and reduces dependencies to fullest extent. This is required to manage the Program Backlog.

3.3. Agile Team

The Contractor shall provide Agile team(s), using Agile Scrum to deliver the solution. The Contractor teams are expected to be high-performing, cross-functional teams. The Contractor shall propose cross-functional teams that will support all application development and operations activities defined in this task. Capacity of a team will be monitored and measured using stories to ensure optimal productivity. The Contractor shall provide

The Contractor will work in a team-based Agile environment and shall provide agile teams to support the Government by completing system backlog items called stories. A story represents any unit of measurable work that provides value to the Government and will serve as a deliverable. The agile teams can work on any system backlog where the stories require the use of the Technical Landscape defined in Appendix G: Technical Landscape or an evolution of the Technical Landscape.

The Contractor shall report metrics for each team. These metrics will be used to assess the performance and quality of the teams and their ability to effectively and efficiently deliver value. At a minimum, the Contractor shall provide the following metrics/reporting for each team: Release burnup, sprint burn down, planned vs accepted story points, escaped defects, and velocity. The teams shall ensure complete transparency and are responsible for logging all activities in the Enterprise Platform (e.g. Jira) and shall be kept current within 1-business day. Contractor shall adhere to Scrum best practices and perform all Scrum Events and Artifacts in accordance with the 2020 Scrum Guide (https://www.scrumguides.org/docs/scrumguide/v2020/2020-Scrum-Guide-

US.pdf).

The Contractor shall provide the number of agile teams and the team composition with the requisite skillset(s) to perform the work described in this task. The Contractor shall identify the total number of teams proposed and the core skillsets must be properly addressed.

The contractor shall

1. Have dedicated team members: A key attribute of Agile teams is that each team can provide the level of work required for sustainment activities associated with Agile development and industry standard System/Software Development Lifecycle, to include providing requirements management, analysis, design, development, test, security and fielding activities.
2. Coordinate all activities (analysis, design, development, testing and deployment) required to complete each story as defined in the Acceptance Criteria and Definition of Done
3. Work with the PO/PM to decompose each story down to the level that is achievable within a sprint (i.e., generally requiring less than 10 business days to complete) and identify the acceptance criteria for each story and define the sprint definition of done.
4. Identify all tasks required to successfully complete each story
5. Show traceability and dependencies between requirements (Epics, Features, Stories, and Tasks) and systems
6. Effectively facilitate scrum and agile events by customizing the facilitation materials based on the nature of the discussion and the audience
7. The Contractor shall ensure the teams' skillsets continue to evolve to keep pace with technology.

The PO/FM will specify high-level requirements/capabilities to the Agile team. In collaboration with the PO, the contractor shall provide stories with the requisite information to complete the work. Working with the PM/PMO/PO, the contractor shall develop and estimate user stories and establish acceptance criteria. The contractor shall ensure these acceptance criteria specify expected functionality for a user story, as well as any non-functional requirements that must be met in the development of the story. No story shall be started by the contractor until approved by the PM/PMO/PO and contain acceptance criteria and a definition of done. A definition of done shall be established and agreed to by both the Government and Contractor at the beginning of each sprint and release cycle. Story approval shall occur at the sprint planning event and shall be documented in the Enterprise Platform (e.g., Jira). The contactor shall ensure story acceptance occurs at the sprint review event and shall be documented in the Enterprise Platform (e.g., Jira). At the sprint review the delivered user stories shall be compared against the definition of done and acceptance criteria defined at sprint planning to determine the quality of the deliverable (story). The Government PO/PM, supported by subject matter experts, will determine whether or not the acceptance criteria have been satisfied. The story shall meet all requirement defined in the sprint definition of done and story acceptance criteria to be accepted.

The Product Owner is the project's key stakeholder and subject matter experts, and supports the PMO. The PO role will be filled by the Government, as the PO is a representative of the needs of the Government user. The PO will be responsible for establishing a vision of what the product team wishes to build and works with the PMO to convey~~ing~~ the vision to the Contractor's scrum or

development team.

The Product Owner's responsibilities include:

- The Product Owner works with the PMO and Contractor to establish and maintain the Product backlog with a complete, prioritized list of features containing descriptions of the desired functionality of the product.
- Providing Clarification on Requirements during Agile Ceremonies: Working with the Scrum Master, end-users, and other subject matter experts, the PMO/Product Owner shall hold recurring backlog refinement sessions to continuously refine and prioritize requirements and decision making during sprint planning and implementation. The PMO (while working with the FM and PO) shall ensure the sprint backlog reflects the highest priority work to be delivered.
- Maintaining Accountability for MVP: The PM/PO/FM shall work with the team to define the MVP.
- Developing, Maintaining, and Assessing Progress Against the Roadmap: The PM/PO/FM shall maintain accountability for identifying the Government requirements for the Product Roadmap, and will identify the capabilities to be delivered by sprint or release. The PM/PO shall review progress after each sprint to assess whether the project is on pace for delivery according to the product roadmap and work with the team to adjust work and schedule as needed.
- Attending Sprint Ceremonies: The PM/PMO/PO shall attend all sprint ceremonies, including the daily Scrums/Stand-ups and the end-of-sprint demonstrations. The PMO/PO shall ensure that the appropriate users are available for the demonstrations to capture appropriate and timely user feedback.
- Holding a User Acceptance Review: The PM/PMO/PO shall work with the COR to inspect and accept / approve Contractor work delivered by each sprint.

The Contractor shall provide a Technical Lead responsible for coordination among the Contractor's development team, the PMO/PO, and the key technical stakeholders to ensure that the technical architecture needs are planned and accounted for in support of the features/capabilities. The contractor shall ensure that Technical Leads maintain a current Secret Clearance, with a current T-3 background investigation, and have Government mandated certifications (Per DoD 8570.01) in addition to the mandated DoD 8570.01 Information Assurance Workforce Improvement Program Information Assurance Technical (IAT) Level III certification.

The contractor's Technical Lead shall:

- Participate in planning, definition, and high-level design of the solution and explore solution alternatives
- Enable the Continuous Delivery Pipeline through appropriate design guidelines
- Actively participate in the Continuous Exploration process as part of the Continuous Delivery Pipeline, especially in identification, planning, and execution of technical work
- Define subsystems and their interfaces, allocate responsibilities to subsystems, understand solution deployment, and communicate requirements for interactions with solution context
- Work with customers, stakeholders, and suppliers to establish high-level solution intent and the solution intent information models and documentation requirements
- Establish critical non-functional requirements

- Support technology/engineering aspects of Program planning and execution
- Provide oversight and foster Built-In Quality and Team and Technical Agility.

The Contractor shall provide personnel capable of the Scrum Master role of Agile Development responsible for facilitating Agile ceremonies and discussions among development and customer team members. There shall be one Scrum Master for every Agile Team. The Scrum Master is responsible for coaching the team on the Scrum processes and removes impediments for the team. The contractor shall ensure the Scum Master role has the knowledge and experience level commensurate for leading Agile teams and perform Scrum Master duties. The contractor shall ensure that Scrum Masters maintain a current Secret Clearance, with a current T-3 background investigation, and have relevant certifications mandated DoD 8570.01 Information Assurance Workforce Improvement Program Information Assurance Technical (IAT) Level II certification.

The Contractor shall provide personnel capable of the Scrum Master role of Agile Development, responsible for facilitating Agile ceremonies and discussions among development and customer team members. The Scrum master role is a requirement for each agile team the contractor develops. This role is responsible for coaching the team on the Scrum processes as well as ensuring efficient team environments. The contractor shall ensure the personnel placed in this role has the knowledge and experience level commensurate for leading Agile teams and in performing Scrum Master duties. The contractor shall ensure that Scrum Masters maintain a current Secret Clearance, with a current T-3 background investigation, and have the mandated DoD 8570.01 Information Assurance Workforce Improvement Program Information Assurance Technical (IAT) Level II certification

The contractor's Scrum Master shall:

- Facilitating Scrum Meetings: The Scrum Master coordinates and facilitates Scrum meetings, such as Sprint planning, Backlog Refinement, Sprint Reviews, and Sprint Retrospectives, and provides sufficient records.
- Defining Team Performance Metrics: The Scrum Master works with product leadership and the team to define and deliver relevant metrics that are formulated and utilized for meeting project objectives.
- Delivering Team Performance Metrics: The Scrum Master works with product leadership and the team to deliver relevant metrics that are formulated and utilized for meeting project objectives.
- Planning and Coordinating Team Training: When appropriate, the Scrum Master shall plan and coordinate training for the team on the Scrum processes. The Scrum Master also helps to remove team roadblocks.

The Contractor shall provide a Project Lead as the primary point of contact for coordination among the Contractor, the PM/PMO/FM/PO, and the Contracting Officer and COR. The contractor shall ensure that Project Leads maintain a current Secret Clearance, with a current T-3 background investigation, and have relevant industry standard certifications.

The contractor's Project Lead's shall:

- Coordinating with the Government PMO to enable timely problem resolution
- Properly aligning staffing requirements
- Facilitating product reporting in line with Agile delivery methods. Per Agile Scrum, the

Contractor's Project Lead will be expected to work with the PM/PMO/PO/FM and Scrum Master to develop Product / Sprint plans and reporting in line with Agile Scrum delivery approaches.

The Contractor shall provide a team member proficient in DevSecOps and who can fulfill AF Cloud One requirement for a contracted team member with Engineering level experience and knowledge accountable for overseeing the continuous integration and delivery (CI/CD) of the working product as required by the Air Force Cloud One office. The contractor's DevSecOps Engineer shall

- Work with the Development, Engineering, Architecture, and Testing teams to define the set of tools and processes for the continuous delivery pipeline
- Work with the contracted Security Lead to ensure that the tools are compliant with security requirements
- Work with the Security Lead to streamline the Authority to Operate (ATO) process from a tools and technical process perspective
- Work with the contracted Testing Lead to automate testing where possible
- Work with the contracted Operations Lead to ensure that the CI/CD processes align with operational requirements.

The member proficient in DevSpecOps shall be highly qualified with extensive demonstrated hands-on experience (commensurate with an Engineering level of knowledge) working with tools and technologies in the following areas: software development, configuration control, testing, security, automation, containerization, orchestration, cloud services, open-source technologies. The contractor shall ensure that DevSecOps Engineer maintain a current Secret Clearance, with a current T-3 background investigation, and have relevant industry standard certifications in addition to the mandated DoD 8570.01 Information Assurance Workforce Improvement Program Information Assurance Technical (IAT) Level III certification.

In accomplishing this task the contractor shall provide the following metrics for each agile team:

- Release Burnup
- Sprint Burn down
- Planned vs Accepted Story Points
- Escaped Defects
- Velocity

3.4. Sprints and Sprint Meetings

The Contractor and the Government will agree upon the duration of Sprints that will suit this effort, ensuring Sprints are kept relatively short (e.g. 2-4 weeks). Once established the duration of individual Sprints shall not be changed, even if the progress is running behind schedule – unfinished items shall be re-inserted into the Product Backlog and prioritized accordingly. The contractor shall be responsible for developing, maintaining, and updating the product backlog and sprint backlog.

At the start of each Sprint, the Contractor shall coordinate with the PMO/PO/PM, the Development Team and the Scrum Master and hold a planning meeting to address the following points:

- the PMO/PM/PO will explain to the Development Team which of the items from the Product Backlog are of a high priority for the current Sprint and the goals and business context for each of those items
- the Contractor shall determine how many of the high-priority items identified by the Government can be developed during the current Sprint.
- the PMO/PO and the Contractor shall review how the "Definition of Done" will be applied to the items to be developed during the Sprint
- the Contractor shall prepare a "Sprint Backlog" specifying for each item to be developed during the Sprint:
  a) a breakdown of that item into individual tasks;
  b) an estimate of the time required to complete each task; and
  c) an allocation of the tasks within the Agile Team.

At the end of each Sprint, the Contractor shall coordinate with the PMO, the Agile Team and the Scrum Master and hold a Sprint Review Meeting at which the items which have been developed during the Sprint will be assessed against the "Definition of Done". The Scrum Master shall be responsible for ensuring that all items presented by the Agile Team at the Sprint review meeting have been completed in accordance with the "Definition of Done".

3.5. Design and Plan

The Contractor shall provide a project plan to the PMO and employ the Scrum process to design the necessary capability. This design shall include all necessary artifacts, with appropriate sizing/complexity documented in the Government ALM, required for planning, development, and testing. The project plan shall include logical milestones (i.e. Epics/Features) for the deployment, which will result in a Minimum Viable Product (MVP), as well as additional functionality and/or enhancements.

3.5.1. Build Planning

For each build, the Contractor shall provide a Build Specification in accordance with a Government provided format. This format may include: (1) Components; (2) Software Assurance (e.g., cybersecurity controls); (3) Build Management, (4) Testing and Integration, and (5) Documentation. The Contractor shall accommodate both routine and out-of-cycle emergency builds. A software maintenance (sustainment) build includes requirements/defect analysis, build planning, software repair, documentation, testing and delivery. The process and approach shall accommodate both routine and out-of-cycle emergency builds.

The Contractor shall support sustainment builds, which may include:

- Reviewing established data naming standards to ensure consistency throughout the AMC enterprise and identifying discrepancies to the Government

- Collaborating with service consumers and maintaining service level agreements (e.g., Web Service Agreements) within available Government repositories, as requested by the Government
- Documenting improved business processes reflected in software maintenance
- Recommending improvements/required changes identified during the software maintenance

The Contractor shall utilize a sustainment build process that:

- Maximizes the number of fixes by minimizing the time to rectify problems
- Minimizes the number of latent defects through effective and efficient testing
- Reduces system risk of unintended consequences when deploying sustainment builds
- Adheres to the testing process described in this PWS

The Contractor shall maintain ongoing interaction and open communication with the PM/PMO/PO throughout maintenance effort. The program specific software maintenance and delivery level of effort for a one-year (1-year) period of performance will not exceed 1,280 story points (10,240 hours) per year for Government-selected CRs, where one story point takes about a day to develop and test; that is, about a half-day to develop and a half-day to test and validate. No refinement hours shall be included in the point value. This can also equate to 4 routine (every three months from a scheduling perspective) and emergency fixes/out-of-cycle releases (when needed) per year, as needed. The content and level of effort for each release will be agreed upon by both developer and government teams, through release planning, before development begins. The level of effort associated with the four (4) software maintenance and delivery categories is defined in Table 1.

Table 1: Maintenance & Delivery Category Level of Effort

	Story Points	Hours	Maintenance
Nano	1	8	Requires a ***"quick fix"*** with no dependencies
Micro	2	16	Requires ***minimal*** changes to a single area of the code base
X-Small	3	24	Requires ***limited*** changes to a narrow portions of the code base, to include, additions or changes to existing columns, metadata or domain data changes to database, changes to existing customize screens
Small	5	40	Requires ***moderate*** changes to more than one areas of selected portions of the code base, to include, new customize screen, advance tool additions or changes, minor changes to existing edit functionality
Medium	10	80	Requires ***significant*** changes to existing lines of code &/or code libraries in a software component & development of several new lines of code, or development of a new software component, to include, basic summary screen, and changes to existing view displays
Large	20	160	Requires ***extensive*** changes to a large portion of the code base, libraries and components and /or of analysis and design with impacts across major portions of the code, design and existing components, complex or advance javascript, , mathematically intense algorithms design/implementation
X-Large (and above)	+/-80	+/-640	Multiple levels of changes related to an entire build/release; varying sizes and level of efforts; X-Large will not be a single work object, but a desired level of effort for a modernized or sustainment deliverable package; this equates to three X-Large for a

			formal build/release

CRs may consist of those requiring no maintenance but documentation changes only. The Contractor shall support two (2) release types: Scheduled (routine) and Out-of-Cycle (OoC) Emergency Maintenance Releases. Out-of-Cycle Emergency maintenance may be delivered and fielded as an Emergency Maintenance Release, as requested by the PM/PMO. Code base of OoC deliveries will be included and delivered as a combined baseline code of the next scheduled release.

In the course of build planning, the Contractor shall perform CM, Quality Assurance (QA), cybersecurity, and documentation for each sustainment build, including:

- Using the SRB CR list for updating and tracking CRs
- Ensuring all maintenance activities (e.g., software updates, COTS upgrades) comply with the current logical and physical architecture - recommended or required deviations shall be presented to the PMO for approval before any further maintenance activities are performed
- Analyzing and providing recommended design and impacts for all CRs provided by the PMO
- De-conflicting and validating all maintenance designs with emerging requirement software development activities, if any (reference optional task for emerging requirements), to ensure compatibility; presenting conflicts for Government decision before any further maintenance activities are performed
- Conducting cybersecurity impact analysis for each CR
- Providing necessary documentation to support security requirements for the build
- Conducting cybersecurity remediation action
- Supporting security control assessment
- Managing multiple versions of software
- Identifying, capturing, and recommending improvements to user business processes and service orchestration supporting those business processes
- Using documented reporting processes to track maintenance progress
- Performing software component and build testing prior to Government Acceptance Testing (GAT)
- Supporting Integration Testing and GAT
- Updating documentation and test cases affected by software maintenance changes

The sustainment build planning process begins after the PO/PM/PMO has determined which CRs will be included in a build, based on recommendations from the contracted development team. As the PMO reviews CRs to determine whether they will be included in a build, the Contractor shall provide support as requested providing related information to the Government. The Contractor shall validate the impact analysis and estimate for each CR, and shall collaborate with the Government to calculate the total point value for the build by using Table 1 above.

As required, the Government may update the build and place some CRs back into backlog. Upon Government acceptance of the initial build specification, the Contractor shall work with the PM Office (PMO) to finalize the Version Release List (VRL) to begin build design execution.

3.6. Build and Deploy

The Contractor shall employ the Scrum process and extreme programming engineering practices to define, build, test, document, and deploy updates to the system using a microservices architecture. This process agility shall support system change frequency for each four (4) week sprint cycle. Each new capability plan shall include checkpoints for milestones to include acceptance for design, build, test, and deploy. Checkpoints are inherent in the Agile development process; however, it is extremely important that new capability software components be uniquely identified during the process. User stories (i.e. functional specifications) shall capture features to be deployed and will be used by the Government as a basis for testing and acceptance.

3.7. Software Defect Support

The Contractor shall immediately respond to escalated production support issues that cause work stoppage or operational problems with the system and ensure the Production system operates without interruption to functional users. Software defects that result in a work stoppage or impact to business operations shall result in an unplanned software hot fix. Correcting defects identified through production support that do not result in a work stoppage shall be prioritized and assigned to current sprint or a future sprint by the Government depending on the impact to business operations. The Contractor shall provide the production support activity in identifying the root cause of production support malfunctions and creating ALM artifacts (i.e. software code changes) to permanently resolve or prevent them. The Contractor shall input all actions taken to resolve artifacts into the Government ALM tool. The Contractor shall coordinate with production support to ensure minimal rework and downtime during software changes, and to ensure the production support activity understands planned system changes.

3.8. Change Management

The Contractor shall facilitate and support configuration management and the administration of the change management process. The Contractor shall create and manage Change Requests (CR) in the change request system (e.g., Jira). In maintaining requirements of sustainment and operational baselines, the Contractor shall follow all applicable configuration management processes and policies as described in this PWS.

The Contractor shall perform requirements analysis for CRs in preparation for future software maintenance builds, collaborating with the Government technical and functional personnel, as needed. The Contractor shall perform CR analysis in accordance with the CR analysis priority list provided by the PO/PMO/PO. The Contractor's completed refinement shall include a story points/development hours for each Epic, Feature, and Story to provide a technical solution for each CR, to include design, code/test, build preparation, and delivery. No refinement hours shall be included in the point value. All story points shall include justification and methodology used to derive the estimate and shall be in sufficient detail to show a complete understanding of the steps required to complete the work. The Contractor's completed refinement also shall include a cybersecurity impact analysis.

In performing the requirements refinement, the Contractor shall:

- Perform in-depth analysis to determine the root cause for end-user issues or data interface anomalies
- Troubleshoot/isolate system problems with internal and external systems/organizations
- Perform an impact assessment of proposed system changes, e.g., imposed by external organization, service providers, interface changes, infrastructure change/operating system (OS) and COTS upgrade, etc.
- Provide estimate the level of effort (i.e. ROM – Rough Order of Magnitude) to implement a system change to include impact, dependencies, high level schedule and story points, scope, and risk

All CRs having successfully completed refinement shall make up the product backlog.
The Contractor shall provide technical input/refinement in the bi-weekly Contractor-led backlog grooming meetings. The government reviews CR refinement, unresolved Help Desk tickets, proposed builds and installs, data quality issues, etc.

The Contractor shall:

- Use the Government-provided change request system
- Maintain the backlog that documents all known requirements, Epics, Features, Stories, and Contractor assigned point values
- Update change requests and re-assess priority as required by the Government
- Brief Government requested change requests and backlog metrics to the ACAS PM or designated Government personnel as requested

The PM/PMO/PO selects CRs for refine from the product backlog, where the contractor shall document all CRs. The Contractor shall refine and assign point values for each CR (with estimate how many hours it will take to complete), and this must be approved by the Government before the PO/PMO prioritizes the CR and determines which CRs will be included in a build or Sprint. The Government may determine some CRs must be built out-of-cycle, in an emergency build. Once the refinement is approved by the Government, and it is validated as an emergency, the Contractor shall begin planning the emergency build.

3.9. Commercial of the Shelf (COTS) Support

The Contractor shall provide support services for changes in COTS and OSS products (e.g. application, operating system, database, application server, web server) to include patches, upgrades, and/or migration to newer technologies. This will involve analyzing the system for incompatibilities and deprecated features. Once prioritized by the Government, the Contractor shall refactor the necessary code to ensure continued system stability. The refactoring shall be assigned to sprint(s) and follow the Agile SDLC process for integration and testing of refactored code.

3.10. DevSecOps and CI/CD Pipeline Support

The Contractor shall provide the expertise required to develop, operate, and maintain a DevSecOps CI/CD pipeline to reliably, repeatably, and efficiently compile, build, test, and deploy code and infrastructure automatically in the Development, Non-Production, and Production environments.

This shall include maintaining virtual machines and components, such as servers, memory, firewalls, load balancers, and storage (i.e. databases). Additionally, the Contractor shall maintain and update the Ports, Protocols, and Services (PPS) and system architecture information. This shall include ports for internal and external traffic as well as the source and destination IP Addresses information. Air Force Department of Defense (AF-DOD) approved PPS worksheet will be used; available on the PPS Management at http://intelshare.intelink.gov/sites/ppsm.

To support this effort, the Contractor shall provide a highly qualified, knowledgeable, and motivate team with extensive demonstrated experience successfully standing up a software delivery pipeline, using a collection of tools and process that enable the DevSecOps pipeline and CI/CD of capability to the user. The Contractor shall establish an organizational software engineering culture and practice that unifies software development (Dev), security (Sec) and operations (Ops). The Contractor shall implement DevSecOps to automate, monitor, and apply security at all phases of the software lifecycle: plan, develop, build, test, release, deliver, deploy, operate, and monitor. Security requirements shall be included upfront to successfully achieve continuous integration and continuous delivery (CI/CD pipeline), continuous monitoring and instrumentation/measurement of working software.

The Contractor shall implement a DevSecOps strategy of the continuous delivery pipeline that aligns with the guidance provided by USTANSCOM and in the DoD Enterprise DevSecOps Reference Design published by the DoD Chief Information Officer. The Contractor will work with the ACAS PMO to increase continuous integration and continuous delivery capability by progressively layering more sophisticated automation components into the continuous integration/continuous delivery pipeline while also reducing the time to move approved code from development to production. In support of this effort, the Contractor shall bring to bear industry and Government practices for elements of DevSecOps such as code repository management, configuration management, branching/merging code, building automation, test code coverage, and automated scanning tools. The Contractor shall look for practices to streamline and integrate security practices within the continuous integration/continuous delivery pipeline that is aligned with USTRANSCOM and the DoD Enterprise DevSecOps initiatives.

The Contactor shall provide the following DevSecOps support:

1) Installation and configuration of application lifecycle management, continuous integration/continuous delivery, and continuous monitoring tools.
2) Design, implementation, and maintenance of the DevSecOps continuous integration/continuous delivery pipeline for cloud and on-premises deployments.
3) Recommending and implementing continuous monitoring industry-based practices.
4) Training and coaching of development teams in utilizing the application lifecycle management and continuous integration/continuous delivery tools.
5) Establishment and maintenance of standards for use of the application lifecycle management and continuous integration/continuous delivery tools.
6) Recommending industry-based practices for incorporating testing, security, and operations representation into the Agile Team early and continuously in the application lifecycle.
7) Recommending industry-based approaches and tools for instrumenting DevSecOps elements to provide greater visibility, transparency and awareness related to pipeline bottlenecks, security and operational issues.

Per the DoD Enterprise DevSecOps Reference Design, the contractor shall provide following capabilities when standing up the DevSecOps and CI/CD capability:

- Use of Open Container Initiative (OCI) compliant and Cloud Native Computing Foundation (CNCF) certified Kubernetes platform to enable interoperability from one Kubernetes installation to the next and allow flexibility to choose between vendors if needed
- Use of hardened containers to maintain security
- Use of the DoD Centralized Artifact Repository (DCAR) to hold the hardened VM images and hardened OCI compliant container images of DevSecOps tools, container security tools and common programming platform components (e.g., COTS or open-source products) that the DoD program software teams can utilize as a baseline to facilitate the authorization process.
- Use of a Sidecar Container Security Stack (SCSS) - A new service that is enabled by DevSecOps and the container-based Kubernetes runtime environment is the Sidecar Container Security Stack (SCSS). This security stack enables correlated and centralized logs, container security, east/west traffic management, a zero-trust model, a whitelist, Role-Based Access Control, continuous monitoring, signature-based continuous scanning using Common Vulnerabilities and Exposures (CVEs), runtime behavior analysis, and container policy enforcement. In addition to the components in the sidecar, there are a few services that support the security sidecar. These include:
    1) Program-specific Log Storage and Retrieval Service
    2) Service Mesh
    3) Program-specific artifact repository
    4) Runtime Behavior Analysis Artificial Intelligence (AI) service
    5) DCAR for the hardened containers
    6) Common Vulnerabilities and Exposures (CVE) Service / host-based security to provide CVEs for the security sidecar container
- The contractor shall be required to work within the USTRANSCOM furnished DevSecOps environment in order to get full source code access, and in order to be able to perform full functional and security tests
- Use DevSecOps and CI/CD pipelines
- Support for automation
    - Development teams developing application code and Infrastructure-as-Code (IaC) to improve quality of integrations, releases and deployments.
    - Security teams strive to automate security by implementing security compliance checking and auditing as code (SaC)
    - Both IaC and SaC are treated as software and go through the rigorous software development and processes including design, development, version control, peer review, static analysis and test
    - Support for continuous and automated testing across the software development lifecycle (Lifecycle phases include - plan; develop; build; test; release; deliver; deploy; operate; monitor)
    - Use DevSecOps and CI/CD pipelines

As the result of accomplishing this task, the contractor shall provide a fully functioning and reusable/promotable blueprints, cookbooks, and DevSecOps pipeline to provide CI/CD, and pipeline design documentation

3.11. Software Assurance and Security Engineering Practice

The Contractor shall provide an expertise in Information Assurance (IA) System Security The IA System Security Lead shall participate in Contractor and Government formal and informal design reviews to identify potential security weaknesses, deficiencies, and/or vulnerabilities in the design. The Contractor IA System Security Lead shall ensure appropriate security requirements are included as part of the requirements traceability matrix and are evaluated as part of the security test and evaluation (ST&E). As part of the Contractor's change control process, the Contractor shall ensure participation by the Contactor IA System Security Lead to evaluate the impact of each change on security. The Contractor shall document the results of this evaluation as part Agile complexity estimate refinement and DevSecOps methodology. The Contractor shall ensure that IA System Security Lead~~,~~ has a current Secret Clearance, with a current T-3 background investigation, and the mandated DoD 8570.01 Information Assurance Workforce Improvement Program Information Assurance Technical (IAT) Level III certification.

3.12. Static Application Security Testing (SAST) Support

The Contractor shall run static code scans on the entire application using a Government approved code scan tool (e.g. Fortify) to scan the developed and changed source code in order to identify and remediate vulnerabilities or weaknesses in the application code, and prevent security vulnerabilities from being deployed into the production environment.

The Contractor shall run static code scans on the container images using a Government approved tool. The Contractor shall ensure vulnerability scanning of container images involves security and operations (IT) teams working in unison throughout the composition and sustainment of custom container build instruction files. The Contractor shall provide vigilant and constant security maintenance of Infrastructure as Code (IaC) scripts and prevent an exploitable infrastructure from being deployed into production.

The contractor shall implement SAST into the automated DevSecOps CI/CD pipeline. The Contractor's Information Assurance System Security Engineer shall analyze code scan results, and ensure findings are remediated or provide rationale on false positives. The Contractor shall deliver the code scan reports to the Government during build execution and build delivery.

As the result of performing this task, the contractor shall perform triage analysis and provide course of action (COAs), test reports, and a DevSecOps CI/CD pipeline containing automated SAST.

3.13. Dynamic Application Security Test (DAST) Support

The Contractor shall run dynamic application code scans on the application using a tool (e.g., Fortify Webinspect, OWASP ZAP, Gauntlt) approved by the Government to from penetration testing of the developed and changed web application to identify and remediate vulnerabilities or weakness in the application and prevent security vulnerabilities from being deployed into the production environment.

The Contractor shall implement DAST in the automated DevSecOps CI/CD pipeline. The Contractor's Information Assurance System Security Engineer shall analyze scan results, and ensure findings are remediated or provide rationale on false positives. The Contractor shall deliver the code scan reports to the Government during build execution and build delivery.

As the result of performing this task, the contractor shall perform triage analysis and provide COAs, test reports, and a DevSecOps CI/CD pipeline containing automated DAST.

3.14. Non-Secure Software

If the Government determines the software delivered under this contract is non-secure, the Government will provide written notice to the contractor of each non-conformity. Software will be "non-secure" under this contract if it contains;

a) a programming error listed on the current approved version of the CWE/SANS TOP 25 (which can be located at https://www.sans.org/top25-software-errors); or
b) a web application security flaw listed on the current approved version of the OWASP Top Ten (which can be located at http://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project); or
c) a security weakness listed in the below severity categories, as defined in DODI 8510.01:
    1) Category I – Vulnerabilities that allow primary security protection to be bypassed, allowing immediate access by unauthorized personnel or unauthorized assumption of super-user privileges; or
    2) Depending on severity as deemed by the Government, Category II – Vulnerabilities that have a potential to lead to unauthorized system access or provide information that have a high potential of giving access to an intruder.

The contractor shall have 15 calendar days after receipt of such notice (Remedy Period) to remedy all non-conformities by modifying/replacing and redelivering the software to the Government; or shall notify the Government within 10 calendar days as to why the remedy cannot be implemented in 15 calendar days and propose a timeline for correction. If the Government determines, after a security audit following a Remedy Period, that the redelivered software is non-secure, and thus non-conforming, the Government may reject the delivery, provide notice of the non-conformance, and document the contractor's performance record. Alternatively, the Government may accept non-conforming software, receive appropriate consideration (equitable price reduction on a fixed price contract, reimbursement for costs of security audit, reimbursement for costs to correct the non-compliances, etc.), and document the contractor's performance record.

3.15. Unit Testing Support

The Contractor shall perform unit testing; testing the smallest unit of testable code isolated from the rest of the software, using a Government approved software tool (e.g. Junit,) to determine if the developed and changed source code functions properly, and prevent code that does not function correct from being deployed into the production environment. The Contractor shall develop test scripts and ensure appropriate logging mechanisms for test results are in place to pinpoint a specific place(s) test automation failure.

The contractor shall implement unit testing into the automated DevSecOps CI/CD pipeline. The Contractor shall analyze the results, and ensure findings are remediated or provide rationale on false positives. The Contractor shall deliver the reports to the Government during build execution and build delivery.

As the result of performing this task, the contractor shall perform triage analysis and provide COAs, test scripts, test reports, and a DevSecOps CI/CD pipeline containing automated Unit Testing.

3.16. Functional Testing Support

The Contractor shall perform automated functional testing using a Government approved software tool (e.g. Selenium, TestComplete, etc.) to determine if the developed and changed source code functions properly and prevent code that does not function correctly from being deployed into the production environment. The Contractor shall develop test scripts and ensure appropriate logging mechanisms for test results are in place to pinpoint a specific place(s) test automation failure.

The contractor shall implement automated functional testing into the automated DevSecOps CI/CD pipeline. The Contractor shall analyze the results, and ensure findings are remediated or provide rationale on false positives. The Contractor shall deliver the reports to the Government during build execution and build delivery.

As the result of performing this task, the contractor shall perform triage analysis and provide COAs, test scripts, test reports, and a DevSecOps CI/CD pipeline containing automated Functional.

3.17. Application Performance and Integration Testing Support

Using a Government approved testing tool, the Contractor shall execute application performance and integration testing on the application after an initial deployment to a staging/test/non-production environment in order to expose issues in non-functional requirements that could not be replicated in the development environments. It should be understood availability issues discovered by application performance testing are in themselves security issues due to a fundamental violation of the Confidentiality, Integrity, and Availability (CIA) triad (availability). Operating and general errors found during testing in the non-production (i.e. Test Findings) will be corrected by the Contractor as work associated with the tested delivery, not new work or additional to the tested delivery. Neither will the test findings be included in the backlog unless Government agrees, based on type or risk level of the error, and required remediation tasks. Government reserves the right to delay acceptance of a release/delivery as based on risk associated with test findings or unresolved issues. The contractor shall address architectural and systems engineering concerns from an availability perspective as early as possible, ensuring that scalability and reliability are built into the architecture and continuously refined.

The contractor shall implement automated application performance and integration testing into the automated DevSecOps CI/CD pipeline. The Contractor shall analyze the results, and ensure findings are remediated. The Contractor shall deliver the application performance and integration test reports to the Government.

As the result of performing this task, the contractor shall perform triage analysis and provide COAs, test reports, and a DevSecOps CI/CD pipeline containing automated application performance and integration testing

3.18. Static Code Analysis and Quality Testing Support

The Contractor shall run static code analysis and quality testing on the application using a Government approved code scanning tool (e.g. SonarQube) to scan the developed and changed source code in order to inspect code quality and identify bugs, code smells, vulnerabilities, and code duplication in the application code, and prevent poor quality and unsecure code from being deployed into the production environment.

The contractor shall implement automated static code analysis and quality testing into the automated DevSecOps CI/CD pipeline. The Contractor shall analyze code scan results, and ensure findings are remediated or provide rationale on false positives. The Contractor shall deliver the code scan reports to the Government during build execution and build delivery.

As the result of performing this task, the contractor shall perform triage analysis, and provide COAs, test reports, and a DevSecOps CI/CD pipeline containing automated static code analysis and quality testing.

3.19. Regression Testing Support

The Contractor shall perform regression testing of the entire system, application, and/or component prior to each deployment to ensure continuing functionality. The Contractor shall perform selected regression tests as part of each capability development and software change to validate software previously developed and tested still performs correctly even after it was changed or interfaced with other software, and that previous capabilities operate properly. Regression testing shall be completed in the pre-production/staging environment and prevent incompatible software from being deployed into the production environment. If a test fails, the Contractor shall analyze and document test data for each component and rework the system and/or application to establish functional equilibrium. The Contractor shall develop scripts and perform testing for the application, database, and operating system in accordance with (IAW) test plans.

The Contractor shall implement regression testing into the automated DevSecOps CI/CD pipeline. The Contractor shall analyze test results, and ensure findings are remediated. The Contractor shall deliver the test reports to the Government during build execution and build delivery.

As the result of performing this task, the contractor shall perform triage analysis, and provide COAs, test scripts, test reports, and a DevSecOps CI/CD pipeline containing automated regression testing.

3.20. Key Performance Parameters and Key System Attributes

The Contractor shall create Features and User Stories for each Key Performance Parameters (KPPs) and Key System Attributes (KSAs) listed in Appendix F. Each KPP and KSA has the measurement,

specific condition, threshold, and objective required to validate performance requirement. Performance Features and User Stories should be executed after each build delivery to determine any performance impacts that must be addressed prior to going to production. After initial delivery of performance Features/User Stories, the Contractor shall deliver performance metrics after each build delivery. All KPPs must be validated, and the performance thresholds documented in performance metrics prior. The Contractor shall deliver the performance metrics to the Government during the build execute and build delivery.

As the result of performing this task, the contractor shall perform triage analysis and provide COAs and performance metrics

3.21. Section 508 Testing

The Contractor shall perform Section 508 testing to ensure requirements have been met. The Contractor shall complete the 508 checklist and provide the document to the Government during build execution and build delivery.

As the result of performing this task, the contractor shall perform triage analysis and provide COAs and Section 508 Checklist.

3.22. DOD Security Requirements Guides (SRGs) and Security Technical Implementation Guides (STIGs) Compliance Support

The Contractor shall register with the DISA STIG library https://cyber.mil/stigs/ to receive notifications for updates and shall ensure the application, supporting application technology (i.e. operating system, database, application servers, web servers, etc.), and environments comply with the most up-to-date version of the DISA SRGs, STIGs, and Application Security and Development STIGs. The Contractor shall remediate any non-compliant checklist items. The Contractor shall enter open STIG findings, along with fix actions, into the Government ALM tool. The contractor shall document compliance in a Security Compliance Checklist for each applicable SRG and STIG using the DISA STIG Viewer tool and deliver the results to the ACAS PMO with each software release.

The contractor shall notify the PM after the contractor is aware ACAS is not in compliance with applicable DISA SRG or STIG. The contractor shall provide a quick-fix recommendation for each DISA SRG or STIG non-compliance items and remediate non-compliant checklist items within 21 calendar days. For non-compliant checklist items that cannot be remediated within 21 calendar days, the Contractor shall mitigate and provide a Plan of Action and Milestone (POA&M) to the ACAS PM to correct the non-compliance. The contractor shall maintain and update the POA&M until compliance is met.

The Contractor Information Assurance System Security Engineering shall participate during any changes to the application, supporting application technology (i.e. operating system, database, application servers, web servers, etc.), system architecture, and environments, to ensure application of all applicable DISA SRGs and STIGs, and National Institute of Standards and Technology (NIST) publications and to identify potential security weaknesses, deficiencies, and/or vulnerabilities. Such modifications shall be made in compliance with all analogous or interfacing

Information Assurance component(s) of the Global Information Grid (GIG) Architecture and shall be designed to make maximum use of the DOD enterprise Information Assurance capabilities and services. As part of the contractor's change control process, the contractor shall ensure participation by the Contractor's Information Assurance System Security Engineer to evaluate the impact of each change on the system's security posture. The contractor shall document the results of this evaluation.

The contractor shall establish an Information Assurance Program to implement and sustain appropriate Information Assurance management, operational, and technical controls and processes required to safeguard DOD non-public information resident on or transiting the contractor's unclassified information systems from unauthorized access and disclosure. Protection measures applied must be commensurate with the risks (i.e. consequences and their probability) of loss, misuse, unauthorized access, or modification of information. The contractor shall submit for Government approval an overarching security plan that describes their strategy for implementation of Information Assurance and Industrial Security requirements throughout the life of the contract. The security plan shall address the security controls described in NIST Special Publication 800-53, Recommended Security Controls for Federal Information Systems and Organizations (http://csrc.nist.gov/publications/PubsSPs.html) and should be tailored in scope and depth appropriate to the effort and the specific unclassified DOD information.

As the result of performing this task, the contractor shall perform triage analysis and provide COAs, STIG Checklist, SRG Checklist, POA&Ms, and the contractor's Information Assurance Program.

3.23. Interoperability and Architecture Support

The contractor shall provide interoperability and architecture support by accomplishing the following tasks:

- Ensure that technical designs and system elements comply with the Defense Information Technology Standards Registry, Defense Information Technology Standards Registry, NIST, DISA, and CCE standards
- Design technical solutions to operate within the ACAS framework, and interoperate with other systems with which ACAS interfaces.
- Ensure technical design and solutions are compatible with DOD infrastructure, e.g., Standard Desktop Configuration, the operational environment, and the CCE.
- Participate in developing and validating Department of Defense Architecture Framework (DoDAF) products. The Contractor shall use AMC Architecture Repository Viewer (ARV) and AMC Enterprise Information Standards Repository suite of tools, also known as Consolidated Architecture Tool Suite, for the source of all DoDAF compliant architectures.
- Use Government reference data source, currently provided by USTRANSCOM Reference Data Management System, as the authoritative source of system reference data.
- The contractor shall maintain the system centric data models which include the Logical Data Model and Physical Data Model IAW USTRANSCOM/AMC Corporate Data Standards and Data Modeling Handbook
- Participate in supporting Air Force, Joint, and Federal agencies certifications.
- Develop prototypes as proof of concepts.

4. Task Area 4: Monitoring and Production Application Support

This task includes, but not limited to, (1) help desk, (2) system, network, and database administration, (3) monitoring, (4) troubleshooting production applications, and (5) responding to incidents that are generated by system users. Production support tickets shall be generated within the Government ALM tool. Production support tickets are the method for tracking and resolving incidents (i.e. specific issues), as well as processing user account requests. Incidents may involve generating software defect artifacts (i.e. for systemic problems requiring code changes); which will be prioritized by the Government. The Contractor shall document incidents and systemic problems for accurate reporting, metrics, and to provide a knowledge base within the Government ALM tool. The Contractor shall be responsible for ensuring the description and resolution for incidents they resolve are documented clearly.

The Contractor shall accomplish the following tasks for the non-production and production environments in the CCE or applicable environment. In the absence of specific contract or Government requirements, the Contractor shall use software and hardware industry standards and industry best practices, which include Capability Maturity Model Integrated (CMMI) for Systems Engineering, Software Engineering, and Integrated Product and Process Development, ITIL®, MIL-STD-100G; Engineering Drawing Practices and ASME Y14.100M; Engineering Drawing Practices. The Contractor shall provide operational support services such as, database administration, systems administration, network administration, version difference training, and help desk support of both legacy and new applications and systems, applications, components, and infrastructure IAW Air Force Instruction (AFI) 33-115 Network Operations and DoD 8570.01M Information Assurance Workforce Improvement Program. Systems operations requirements must comply with applicable documents and standards specified in Section 8 of this PWS.

The contractor shall provide the support services necessary to operate and maintain ACAS IAW Government provided configuration baseline, operational performance and availability requirements, and recommended original equipment manufacturer (OEM) operation and maintenance procedures. The Contractor shall meet a system operation and availability requirements, Threshold 99% Objective 100%, with a cumulative downtime not greater than 10 minutes per month, except for Government approved scheduled downtime, to meet ACAS RMF CIA categorization M-M-H.

System availability is defined as the total time the system as a whole is available to users. The "whole" system includes both system availability and data availability. ACAS currently has redundancy and users can be redirected to other enclaves in the event an enclave goes down. In this case, the amount of time required to transition users from the affected system to the redundant system will count against the allowable downtime for the affected system each month. Data availability covers three areas: replication and information services and interfaces. Replication is a measure of data latency. Information services and interfaces are measures of data availability which directly impact the whole system for the user.

As the result of performing this task, the contractor shall provide

- **System Performance Report**. This report shall contain all open tickets listed in order of

priority starting with highest priority, and further sorted such that the earliest ticket of a given priority is at the top for that priority grouping. This report shall contain the ticket #, priority, associated tickets, descriptions, corrective action, date opened and closed with the user, as well as trend and other pertinent data. It shall correlate actions taken to other tasks or solutions that resolved similar tickets. If the Contractor has detected a trend, this report shall include a brief summary of the trend, associated tickets, pertinent distribution of causes, and recommended corrective action to prevent similar troubles. The Contractor shall use their expertise to recommend changes to software code, queries, data validations, etc. The Government will review these recommendations and provide guidance when appropriate. Since the production support tickets are managed via the Government ALM tool, metrics associated with responsiveness, quantity, and duration of tickets shall be extracted directly from the ALM tool and summarized in the report.

- **Cyber Intrusion Incident Report**. This report shall provide details identifying the root cause, impacts, and actions taken to resolve and prevent the vulnerabilities. The Initial Cyber Intrusion Incident Report is due within four (4) hours of the event. The Cyber Intrusion Incident Report Update is due within twenty-four (24) hours of the event.

4.1. Client Support Technician (CST)/Functional System Administrator (FSA) Support Work-Center Environment Administration Support (EAS)

The Contractor shall provide CST/FSA/EAS assistance in support of the contract environments in accordance with AFI 33-115v1, Network Operations. The CST/FSA/EAS area of support consists of the environments and workstations used by the Contractor.

In order to ensure that Contractor personnel have adequate permissions to provide the CST/FSA/EAS, the Contractor shall request access authorization in writing. This request shall contain an explanation of the need for the permissions, the equipment requiring the permissions, the type of permissions required, and the name of the person(s) to include his or her email address, work phone number, and evidence that the individual(s) has the requisite certification in accordance with DoD 8570.01-M, Information Assurance Workforce Improvement Program. The written request is to be delivered to the COR or appropriate Government agency. The contractor shall ensure that CST/FSA/EAS personnel have relevant industry standard certifications in addition to the mandated DoD 8570.01 Information Assurance Workforce Improvement Program Information Assurance Technical (IAT) Level II certification.

4.2. Functional and Technical Help Desk Support

The Contractor shall provide Functional and Technical Help Desk Support. In providing help desk support, the Contractor shall utilize a team of individuals with a working knowledge of and who display expert qualifications for the functions and operations of the application, supporting application technology (i.e. operating system, database, application servers, web servers, etc.), networks, and environments as well as knowledge of call tracking applications, experience, and training in customer service. Help Desk services shall be 24 hours per day, 7 days per week, 365 days per year (24x7x365). The contractor shall ensure that help desk personnel have the mandated DoD 8570.01 Information Assurance Workforce Improvement Program Information Assurance

Technical (IAT) Level II certification.

The Contractor shall develop and implement Help Desk metrics to enable the identification of trends in user problems, functional deficiencies and design deficiencies, other technical issues and Help Desk process issues. Working with the Government, the Contractor shall use these metrics to analyze and recommend solutions to improve supportability and maintainability for system capabilities and continually improve the Help Desk process. The contractor shall provide a summary of the problem management Help Desk activities in the Help Desk Report as part of the Monthly Status Report (MSR) and shall include support provided to end users, tickets received and closed, status of open tickets, and any trends identifying common user/technical problems, significant sustainment actions and recommendations for improvement and Help Desk metrics. The contractor shall provide Help Desk scripts and supporting material to allow for Level 1 support of system capabilities. Problem management shall be responsible for reporting Cloud Service Provider (CSP) outages and coordinating CSP outages with appropriate incident management personnel. The contractor shall assist in troubleshooting issues related CSP outages impacting system availability.

The Contractor shall provide the following functional assistance:

- explaining technical solutions needed to accommodate business processes
- assisting user communities with software functionality relating to their business processes/software processing
- accomplishing user training,
- validating the business operation rationale of correct software operations
- explaining to program and government representatives or their designated personnel the software's user functionality

The Contractor shall update help desk tickets as follows:

- High Priority Tickets – Update hourly until resolved
- Medium Priority Tickets – Update daily until resolved
- Low Priority Tickets – Update weekly until resolved

The Contractor shall:

- Respond to requests for functional or technical assistance in person, via phone, electronically, and walk-in
- Monitor Systems' operations and respond to faults, alarms, abnormalities, or potential issues
- Diagnose and resolve functional application or technical software issues
- Research questions using available information resources
- Advise user on appropriate action
- Create, change, and delete user accounts per request. This subtask further includes:
  - password issuance & resets
  - user authentication provisioning and support
  - establish and modify permissions
  - monitor and respond to requests for new accounts using customer requesting systems (e.g. trouble tickets tracking system)
  - establish and maintain a log of accounts and account status
  - obtain account access approval when users request non-standard privileges
  - Ensure account request documentation is complete and accurate IAW the respective

program's account management processes
    - Monitor account usage in order to lock and delete accounts based on current security regulation and/or individual program guidance
- Validate and authenticate all user accounts to ensure only authorized users have account access annually or when required by an applicable Notice to Airman (NOTAM), or according to AMC/A6 or AMC/A3B guidance
- Advise user on appropriate action:
    - Redirect problems to appropriate resources
    - Identify and escalate situations requiring urgent attention
    - Ensure trouble tickets are documented in the trouble ticket tracking system (TTTS) and protected according to classification level
    - Track and route problems, requests, and document resolutions
    - Track and monitor all customer support requests and troubleshooting and resolution actions in the TTTS
    - Provide final trouble ticket closeout by identifying what the actual issue was and how it was it resolved in the TTTS
    - Notify appropriate authorities when a trouble ticket becomes Operations Reportable (OR) (e.g. System failures and other situations where System degradation and/or outage is observed or reported) IAW System OR Criteria
- Research questions using available Information Resources
- Stay current with system information, changes and updates
- Administer, maintain, and modernize automated tools required to sustain Help Desk operations
- Monitor Systems' operations and respond to faults, alarms, abnormalities, or potential issues
- Diagnose and resolve technical system and software issues
- Administer Help Desk software
- Redirect problems to appropriate resource
- Identify and escalate situations requiring urgent attention
- Track and monitor all customer support requests, troubleshooting and resolution actions
- Ensure trouble tickets are documented in the TTTS and protected according to classification level and authenticate all user accounts to ensure only authorized users have account access annually or when required by an applicable Notice to Airman (NOTAM), or according to AMC/A6 or AMC/A3B guidance
- Document and provide the status of trouble tickets when requested by Government entities
- Track and route problems, requests, and document resolutions
- Prepare activity reports

The Trouble Ticket Tracking System will be used for passing troubleshooting information from Level 1 or 2 to Level 3 Help Desk.

Level 1 – Applies basic knowledge of Information Technology (IT) concepts, practices and procedures within the environment.
Level 2 – Applies knowledge and experience with standard IT concepts, practices, and procedures within the environment.
Level 3 – Expert in all functions of both Level 1 and Level 2 positions. Applies extensive knowledge of a variety of IT field's concepts, practices, and procedures to ensure the secure

integration and operation of all enclave systems.

As a result of performing this task, the contractor shall provide a Service Desk Report (as part of the MSR), Service Desk Metrics (as part of the MSR: number/type of incidents; average time to resolve; age of unresolved incidents, etc), and enter Change Requests (for problem resolution) in the Enterprise Platform (e.g. Jira).

4.3. System Administration Support

The Contractor shall provide 24x7x365 expert system administration services for ACAS in the CCE . These services consist of system/servers provisioning, installation, configuration, operation, and maintenance of Systems servers, software, and related infrastructure. These services consist of performing multiple, highly complex, technical tasks with routine upgrades in order to meet a changing production environment, applications, system designs, configurations, servers, utilities, and operational conditions. The Contractor shall ensure the application, supporting application technology (i.e. operating system, database, application servers, web servers, etc.), networks, environments and related procedures adhere to government approved configurations; government system availability and reliability standards; and OEM system operation and maintenance procedures. The contractor shall document all procedures in the Contractor Maintained Procedures.

The Contractor shall provide a wide range system administration services which may include, installing, supporting, and maintaining servers or other computer systems, planning for and responding to service outages and other problems. The Contractor shall quickly and correctly diagnose software failures and follow through to resolution. The Contractor shall assist in the prevention of computer hacking and other security problems by implementing preventive measures in compliance with DOD, USTRANSCOM, and AF guidelines. The Contractor shall ensure all firewalls and intrusion detection or other information assurance systems are fully functioning as intended and are kept current. The Contractor shall monitor the performance of the system(s), application(s), component(s), infrastructure and resolve any issues related to the efficient and effective use of the system in general. The Contractor shall support the Government in addressing contingent and emergent IT system outage conditions with any necessary services until resolution of the condition. This support may extend to relocation, reallocation, replacement, or reconstruction of IT systems, components, applications, infrastructure and software. The contractor shall ensure that system administration personnel maintain a current Secret Clearance, with a current T-3 background investigation, and have relevant industry standard certifications in addition to the mandated DoD 8570.01 Information Assurance Workforce Improvement Program Information Assurance Technical (IAT) Level II certification.

The following is a listing of system administration functions that shall be performed by the Contractor:

- Perform system monitoring including monitor alarms; verify the integrity and availability of all interfaces, server (including virtual server) resources (e.g., Central Processing Unit (CPU), memory, disk space utilization, disk I/O, etc.), systems, and key processes; review system and application logs; use system-provided dashboards/control panels to perform regular, in-depth monitoring, and verify and document completion of scheduled jobs (e.g. data loads, clean-up scripts, backups, and resets.)

- Maintain configuration and awareness of virtual environment, including number and type of virtual servers, applications running on those servers, and activate, move, and close applications running on virtual servers.
- Perform regular security event monitoring to identify any possible intrusions
- Perform backup operations, ensuring all required file systems and system data are successfully backed up to the appropriate media, recovery tapes, disks, drives and utilities are created, and media is recycled and sent off site as necessary
- Perform regular file archival and purging as necessary
- Repair and recover from software failures
- Coordinate and communicate with System Manager and impacted constituencies for activities, (e.g. system maintenance, System failures, and other situations where system degradation and/or outage may occur) to facilitate Authorized Service Interruption (ASI) scheduling
- Lead troubleshooting teleconferences with users, support, and development personnel to resolve open system issues as documented in the TTTS
- Notify appropriate authorities when a trouble ticket becomes OR (e.g. System failures and other situations where System degradation and/or outage is observed or reported) IAW Systems' OR Criteria
- Review, install, verify and document all OS patches and upgrades; upgrade administrative tools and utilities; and apply Time Compliance Network Order (TCNO), Information Assurance Vulnerability Management (IAVM), and other downward directed security patches
- Review scans following patch/upgrade application to ensure successful and open trouble tickets for any system security findings identified during the scan
- Configure/add new services as necessary as directed by the system
- Upgrade and configure System software that supports infrastructure applications according to project or operational needs including new software releases, hotfixes, and patches
- Perform software fielding in accordance with software version document releasing instructions, and/or COR instructions, ensuring the correct version of software delivered from the production Configuration Management Library is loaded
- Maintain operational, configuration, or other procedures
- Maintain a knowledge base of problems and solutions including troubleshooting techniques, fix actions, and applicable procedures and document them in a Contractor Maintained Procedures
- Monitor, maintain, and ensure currency of server certificates
- Provide a monthly report of all server certificates, to include server name, certificate expiration date, and actions needed to obtain new certificates
- Provide performance reporting to support capacity planning
- Perform ongoing performance tuning, upgrades, and resource optimization as required
- Configure CPU, memory, virtual servers and images, and disk partitions as required following instructions provided by the systems
- Solve technical issues with web server, database server, applications server, virtual server, Domain Name Service (DNS), Simple Mail Transfer Protocol (SMTP), appliances, utilities, or other System software
- Propose software or server updates and other systems enhancements to improve systems performance and reliability; schedule and coordinate level-appropriate maintenance

- Troubleshoot and resolve systems service and OS-level issues, plus issues referred by system managers, program offices, the help desk, database managers, systems engineers, systems administrators, and other technicians
- Provide advanced troubleshooting skills and the ability to rapidly identify issues and provide restoration of issues
- Keep detailed records/logs of work activities/system performance to support metrics and reporting and include in Monthly Status Report
- Participate in fault isolation, detection, and correction relative to the Systems at host sites and interfaces
- Log all user access requests in the TTTS
- Interpret System practices, diagrams, specifications, drawings, and service orders
- Prepare system inputs, analyze system outputs, and maintain and repair various electronic systems
- Install, maintain, upgrade, modify, isolate and repair System server, and system software
- Coordinate and implement software code upgrades
- Coordinate and implement installation of new servers and products
- Coordinate all maintenance actions and schedule System outages with System representatives
- Ensure full data and system recovery to operational status upon completion of maintenance and/or recovery actions
- Provide after action notification describing maintenance actions to the M/ACCC.
- Monitor user load balance, for System with load balancing capability, and adjust and direct users to alternate sites as required
- Create and maintain scripts for task automation
- Assist in the operational validation of application updates, enhancements and changes for the purpose of ensuring applications and related systems function appropriately and meets configuration baseline and database software requirements
- Track and monitor all customer support requests and troubleshooting and resolution actions in the Trouble Ticket Tracking System
- Ensure trouble tickets are documented and protected according to classification level
- Ensure final closed trouble ticket accurately reflects what the actual issue was and how it was resolved
- Identify and report items that are incorrectly identified in the configuration baseline or missing from the production configuration documents
- Support tracking, coordination, and reporting on TCNOs, Information Assurance Vulnerability Alert (IAVAs), and other downward directed security patches
- Provide technical administration and environment support services to the production and non-production environments.
- Coordinate all scheduled maintenance outages with appropriate agencies.
- Execute performance tuning.
- In observation of AF, USTRANSCOM and DoD policies, maintain, update, and exercise system Contingency Plans/Continuity of Operations Plans (COOPs) and environments according to the prescribed schedule mandated by the system's Risk Management Framework (RMF) Availability Level.
- Verify the capability of existing servers to accommodate the application changes; identifying

the need to acquire/change/additional COTS software, or software licenses, recommending any infrastructure changes necessary; validating the fielding schedule.
- Support Project Support Agreement efforts.
- Coordinate and execute installation and fielding of delivered products, hotfixes, and upgrades.
- Develop and provide detailed fielding plan for all fielding activities and identify / coordinate outages.
- Field only approved PBLs.
- Ensure all PBL software and documentation used in the fielding is obtained ONLY from configuration management,
- Develop and provide to the Government operations and troubleshooting procedures
- Monitor, respond to, and update trouble tickets as appropriate. Provide ad-hoc trend analysis of tickets.
- Recommend and provide analysis of production performance metrics.
- Coordinate all system, application, component, infrastructure problem(s) and outage resolution activities with relevant agencies and offices and provide detailed documentation upon their resolution.
- Ensure identified requirements for the non-production and production environments are captured, documented, and verified prior to the required event.
- Assess performance of new products in conjunction with stakeholders; provide analysis and recommendations in preparation for product/release fielding determination.
- Provide technical administration of environments utilizing Government-authorized tools and methods.
- Monitor and maintain system, application, components, infrastructure backups and libraries.
- Maintain configuration control of all environments.
- Perform system, application, component, infrastructure and software monitoring, as well as performance tuning.
- Ensure the environments are in operational state prior to the scheduled event requiring its availability.
- Maintain load balancing and fail over procedures utilizing provided tools.
- Analyze, plan, and recommend system, application, component, infrastructure requirements and timing for the insertion of new technology.
- Prepare or modify architecture, updating the architectural drawings.
- Perform technical software update, upgrade, or refresh in order to maintain environment currency.
- Annually or as requested by the ACAS PM, prepare 18-month forward-looking Technology Refresh Plan, to include software, infrastructure, and configuration changes; project impact to the systems, applications and components.
- Prepare, review, and update architectural diagrams, and environmental service diagrams for all operating locations. Diagrams shall be reviewed at least annually to determine accuracy.

4.4. Network Administration Support

The Contractor shall provide 24x7x365 network administration services for ACAS in the CCE. The contractor shall provide network administration services consisting of network/appliance

provisioning, installation, configuration, security, operation, and maintenance of Systems servers, software, and related infrastructure. This includes all related local area and wide area networks or segments, data communications, and associated servers, software, and appliances within the applicable production environment(s). These services consist of performing multiple, highly complex, technical tasks with a need to routinely upgrade skills in order to meet a changing production environment, applications, system designs, configurations, utilities, and operational conditions. The contractor shall ensure the Systems servers, OS, software systems, and related procedures adhere to Government approved production configurations; Government system availability and reliability standards; and OEM system operation and maintenance procedures. The contractor shall document all procedures in the Contractor Maintained Procedures. The contractor shall ensure that network administration personnel have relevant industry standard certifications in addition to the mandated DoD 8570.01 Information Assurance Workforce Improvement Program Information Assurance Technical (IAT) Level II certification.

The following is a listing of system and network administration functions that shall be performed by the contractor:

- perform network monitoring including monitoring alarms; verify the integrity and availability of all hardware, appliances, resources, and systems
- Perform regular security event monitoring to identify any possible intrusions
- Repair and recover from software failures
- Coordinate and communicate with System Manager and impacted constituencies for activities (e.g. System maintenance and other situations where System degradation and/or outage may occur) to facilitate ASI scheduling
- Lead troubleshooting teleconferences with users, support, and development personnel to resolve open system issues as documented in the TTTS
- Notify appropriate authorities when a trouble ticket becomes OR (e.g. System failures and other situations where System degradation and/or outage is observed or reported) IAW Systems' OR Criteria
- Review, install, verify and document all OS patches and upgrades; upgrade administrative tools and utilities; and apply TCNO, IAVM, and other downward directed security patches
- Upgrade and configure network software that supports infrastructure applications according to project or operational needs
- Perform a pre-fielding review of software and hardware fielding documentation and identify any clarifications prior to starting a fielding activity in the TTTS
- Perform software fielding IAW software version document releasing instructions provided by support and development organizations
- Maintain all procedures associated with sustaining the production environment and document them in Contractor Maintained Procedures
- Maintain a knowledge base of problems and solutions including troubleshooting techniques, fix actions, and applicable procedures and document them in Contractor Maintained Procedures
- Monitor, maintain, and ensure currency of network device/appliance certificates
- Provide performance reporting to support capacity planning
- Perform ongoing performance tuning, hardware upgrades, and resource optimization as required

- Maintain the network environmental and monitoring equipment
- Solve technical issues with network appliances, utilities, or other network software
- Propose software updates and other network enhancements to improve systems performance and reliability; schedule and coordinate level-appropriate maintenance
- Troubleshoot and resolve network service issues, including issues referred by System Managers, program offices, the Help Desk, database managers, network engineers, systems administrators, and other technicians
- Provide advanced troubleshooting skills and the ability to rapidly identify issues and provide restoration of issues
- Provide rapid restoration of network anomalies including assistance with disaster recovery of the network
- Identify, test, diagnose, and analyze troubles in the network
- Keep detailed records/logs of work activities/system performance to support Metrics and Reporting and include in Month Status Reports
- Initiate, process, and track requests for firewall configuration changes and firewall configuration waivers when a customer with established System accounts requires network access and assistance
- Troubleshoot end-to-end network connectivity issues affecting the operations and performance of systems
- Operate and maintain program specific Virtual Private Networks and firewalls and other network appliances
- When end-to-end network connectivity and network access issues arise relative to the System at host sites, interfaces, or at other locations in the US or overseas, participate in the fault isolation, detection, and correction; coordinate repair efforts; and track status
- Log all user network access requests in the TTTS
- Interpret network practices, diagrams, specifications, drawings, and service orders
- Prepare system inputs, analyze system outputs, and maintain and repair various electronic systems
- Install, maintain, upgrade, modify, isolate and repair network devices, appliances, and System software/hardware
- Provide support for the management of the network and performance of duties related to the operation of the network, including change management and problem resolution
- Coordinate and implement installation of products in the network
- Coordinate all maintenance actions and schedule System outages with the System Manager
- Collate and document the necessary information (problem, troubleshooting steps taken, stakeholders coordinated with etc.) for creating requests for higher-level technical support
- Ensure full availability and security to operational status upon completion of maintenance and/or recovery actions. Status shall be confirmed using two person integrity as a control mechanism
- Execute after action notification procedures describing maintenance actions to the MCCC for ASI and OR events
- Monitor user load balance and adjust and direct users to alternate sites/enclaves
- Track and monitor all customer support requests and troubleshooting and resolution actions in the TTTS

- Ensure trouble tickets are documented in the TTTS and protected according to classification level
- Provide final trouble ticket closeout by identifying what the actual issue was and how it was resolved in the TTTS
- Support the modernization, technology insertion, performance analysis and turning, maintenance, testing, migration and integration of the System into a DoD or commercial cloud environment (such as IaaS and Amazon Cloud)
- Identify and report items that are incorrectly identified in the configuration baseline or missing from the production configuration documents
- Support tracking, coordination, and reporting on TCNOs, IAVAs, and other downward directed security patches

4.5. Database Administration Support

The Contractor shall provide 24x7x365 database administration services for ACAS in the CCE. These services consist of performing multiple, highly complex, technical tasks with a need to routinely upgrade skills in order to meet changing database applications, system designs, and production environment conditions. Specific skill-based competencies are required to satisfactorily perform this task, which are the interaction and data transfer between hosts and clients, preparing and maintaining accurate records, and utilizing the functionality of pertinent software applications. Due to the rapidly evolving nature of IT, the Contractor shall keep pace with system and operational environment changes by ensuring it has the appropriate skill set to effectively perform the database administration task without delay and/or system degradation. The Contractor shall provide database administration support for logical and physical database designs. The Contractor shall create and test backups of data, provide data cleansing services, provide performance tuning and active monitoring, verify data integrity, implement access controls to the data, ensuring maximum availability and performance within the non-production and production environment. The Contractor shall develop data exposure services to efficiency and effectively use the database. The contractor shall ensure that database administration personnel maintain a current Secret Clearance, with a current T-3 background investigation, and have relevant industry standard certifications in addition to the mandated DoD 8570.01 Information Assurance Workforce Improvement Program Information Assurance Technical (IAT) Level II certification. The Contractor shall ensure the database administrator have can maintain an Oracle Database at a level of 24/7/365 with minimal downtime, and maintaining Database security and PL/SQL. portions ɵf the system.

The following is a listing of database administration functions that shall be performed by the Contractor:

- troubleshoot and resolve database system malfunctions to meet operational parameters and resolve issues by detecting and isolating faults, and taking corrective action to restore to fully operational status
- upgrade databases for the purpose of ensuring their ability to use new and/or existing databases and related software
- ensure all issues and outages are properly documented in the Trouble Ticket Tracking System or other government directed location
- analyze and sustain capacity and performance requirements

- analyze, consolidate, and tune databases for optimal efficiency
- monitor systems and platforms for availability and database systems serviceability
- back-up, replicate, and failover assigned databases
- restore and recover corrupted databases
- ensure database systems are configured to meet security directives
- build database servers, install, and configure database software on servers
- perform database dumps, table maintenance, re-indexing, and database replication maintenance in accordance with industry standards and/or the applicable database maintenance guidance
- install patches for applicable database software
- execute and monitor regular and ad hoc job execution in databases
- consult with software application developers on preparing SQL queries and effective use of features and options of the applicable database software
- consult with engineers and application developers on existing and potential performance parameters, to include identifying and resolving performance issues
- resolve problems and meet user needs and system operational and functional requirements
- assist in the operational validation of application updates, enhancements and changes for the purpose ensuring applications and related systems function appropriately and meets configuration baseline and database software requirements
- coordinate database activities (e.g. security, upgrading, populating, refreshing, repairing database systems, cataloging, access rights, etc.) for the purpose of ensuring data accuracy and availability
- monitor compliance with DoD and US Air Force database security, integrity, and Personally Identifiable Information protection standards and procedures
- using a variety of database support processes, ensure the operation, stability and performance of the production databases and the availability of stored data
- monitor assigned applications and related systems for the purpose of reducing application downtime and ensuring that assigned applications are available when needed to meet system performance and availability parameters
- enforce database schemas, tables, procedures, and permissions
- set up data sharing according to configuration
- create and maintain scripts for task automation
- update operationally required data imports from approved sources and data extracts required to support operational needs
- create, delete, and modify database user and privileged user accounts and access privileges
- notify appropriate authorities when a trouble ticket becomes Operations Reportable (OR) in accordance with Systems' Operations Reportable (OR) Criteria
- track and monitor all customer support requests and troubleshooting and resolution actions in the Trouble Ticket Tracking System
- ensure trouble tickets are documented and protected according to classification level
- ensure final closed trouble ticket accurately reflects what the actual issue was and how it was it resolved
- ensure that the software loaded on supported systems is the correct version from the software delivered from the production Configuration Management Library
- identify and report items that are incorrectly identified in the configuration baseline or missing from the production configuration documents
- support tracking, coordination, and reporting on TCNOs, IAVAs, and other downward

directed security patches

4.6. Monitoring Support

The contractor shall develop a risk management approach to cybersecurity that maintains an accurate picture of ACAS's security risk posture, provides visibility into assets, and leverages use of automated data feeds to quantify risk, ensure effectiveness of security controls, and implement prioritized remedies. The Contractor shall provide a well-designed continuous risk management process to transform risk assessment and monitoring from a static activity to a continual monitoring activity that is enabled by automated processes and tools.

The Contractor's continuous monitoring shall be an extension to continuous operation, and continuously inventories all system components, monitors the performance and security of all components, and logs application and system events.

The Contractor shall utilize automated tools where available to collect and assess key information about the use of the application to discover trends and identify problem areas. Monitoring activities shall span the underlying computer resources, storage, network transport, applications / microservices, containers, interfaces, normal and anomalous endpoint behavior, and security event log analysis. It will also include behavior and signature-based detection in the runtime environment. All these security capabilities will be mapped against the NIST controls and follow NIST Special Publication 800-190 Application Container Security Guide for continuous compliance.

The Contractor shall monitor current health, performance statistics, recent errors, full logs, and key metrics. The Contractor shall ensure the system is working normally; and report and resolve any breaches, security attacks, or anomalies in activity. The Contractor shall use log collection, monitoring, and analysis to understand the relationship between network, infrastructure, servers, application framework, and user behavior to gain a comprehensive view across all activity, across all sources, servers, and locations. In the event of a Cyber incident or intrusion, the contractor shall conform to the policy outlined in the ACAS Incident Response Plan. The Contractor shall report any detected cyber intrusions. Cyber incidents shall be documented in a Cyber Intrusion Incident Report. The incident report shall document and report loss/compromise, suspected compromise, suspicious contact, or activity involving systems accredited to process classified information. It may be used as a preliminary response to supplement national reporting requirements and provide a resource to document initial or first response to a Cyber incident.

The Contractor shall perform the following activities:

- Logging: Log system events, to include, all users, network, application, and data activity
- Log analysis & auditing: Filter or aggregate logs; analyze and correlate logs; and providing remediation reports.
- System performance monitoring: Monitor servers, software, database, and network performance; baselining system performance; detect anomalies; and providing recommended actions
- System Security monitoring: Monitor security of all system components; security vulnerability assessment; system security compliance scan; providing vulnerability

incompliance findings, assessments, and recommendations.
- Asset Inventory: Inventory system IT assets
- System configuration monitoring: System configuration (infrastructure components and software) compliance checking, analysis, and reporting; provide compliance report and recommended actions
- Database monitoring and security auditing: Database performance and activities monitoring and auditing, to include, database traffic, event, and activities.

4.7. Production Support

The Contractor shall respond to and resolve operational problems with the system. This task includes responding to incidents, analyzing and correcting specific incidents, creating software development artifacts for systemic problems requiring code changes, and following escalated tickets to resolution. Typical incidents to be resolved under this task include database updates for specific records with incorrect data, which involves determining the cause of the issue, correcting the database, and determining whether a permanent code fix is necessary.

4.8. Production Support Analysis

The Contractor shall analyze problems and solutions to detect and report trends and "worst actor" features and/or processes. These recommendations shall consider the simplest solutions first. For example, a trend in user errors for entering data might be solved by adding help text or changing data validations. On the other hand, recurring errors may require changes to functionality or the database. The Contractor's expertise must be sufficient to support such analysis and to provide concise, actionable recommendations. For complex recommendations, the Contractor may have to collaborate with the Government or other Contractor personnel to create change specifications. Support analysis may also result in recommending changes to system documentation or training material.

4.9. Cybersecurity Analysis

The Contractor must be cognizant of the dynamic nature of security and Information Assurance activities and plan to support these efforts with the initiative and sense of urgency it demands. The Contractor shall monitor, acknowledge, evaluate, analyze, test and provide course of action ensuring compliance with TASKORDs, IAVM Notices, IAVA, Air Force Computer Emergency Response Team, Time Compliance Network Orders (TCNO), USTRANSCOM Security Notifications, United States Computer Emergency Readiness Team, Technical Analysis & Response Cell Security Notifications, USCYBERCOM Security Notifications, vendor security advisories, and other security vulnerabilities, assessments, and requirements. The Contractor shall determine system impact, identify mitigating factors, and provide recommendations to the Government regarding potential courses of action. The Contractor's recommendations shall be compliant with DOD security requirements and industry best security practices. The Contractor shall ensure that cybersecurity remediation, patch deployments, and other significant security activities are considered in the Product Roadmap. The Contract shall complete the monthly Cyber Hygiene Scorecard.

The contractor shall:

- Notify the ACAS PM after the contractor determines ACAS compliance or non-compliance with the security notification.
- Create and provide compliance instructions to execute on all supported environments.
- Track progress for reporting purposes and provide weekly status updates to the ACAS PM.
- Mitigate all CAT I vulnerabilities within 7 calendar days of identification.
- Initiate POA&M for CAT I vulnerabilities that cannot be mitigated within the 7 calendar day timeframe.
- Initiate a POA&M for non-CAT I vulnerabilities that cannot be mitigated within a 21 day timeframe.
- Provide a POA&M to the ACAS PM in the event the corrective action required for compliancy cannot be implemented by the suspense date established in the security notification.
- Maintain and update POA&Ms until ACAS is compliant with the security notification.
- Collaborate with the Government's designated Information Assurance Office, currently designated as 375 CSPTS/SCCA, regarding test, operation, monitoring, and support of all security and IA products, services, and controls.

The contractor shall ensure that Information Assurance System Security Engineer personnel maintain a current Secret Clearance, with a current T-3 background investigation, and have relevant industry standard certifications in addition to the mandated DoD 8570.01 Information Assurance Workforce Improvement Program Information Assurance Technical (IAT) Level III certification.

As the result of the task, the contractor shall perform triage analysis, provide COAs, Compliance Tracking and Progress Report, POA&Ms, and complete Cyber Hygiene Scorecards.

4.10. Cybersecurity Service Provider (CSSP) Support

The Contractor shall provide Host Based Security System (HBSS) and Assured Compliance Assessment Solution (ACAS) scans weekly; and shall participate in one (1) COOP exercise (i.e. Intrusion Assessment or Incident Response) annually.

The Contractor shall assume the following HBSS (or its successor) responsibilities for all ACAS environments

For Production cloud environment, the Contractor shall:

- Perform application administration in concert with Government's designated Information Assurance Office.
- Perform System Production, Installation, Operation & Maintenance activities on approved HBSS Change Orders.
- For Non-Production cloud environment, the Contractor shall:
- Maintain and operate HBSS Management console.
- Validate HBSS Change Orders issued by Higher Headquarters against all systems, applications, and/or components in order to assess impact to ACAS Mission Readiness.
- If Change Order should not be applied, the Contractor shall provide rationale to ACAS PM to facilitate feedback to higher headquarters.

4.11. Interoperability Testing and Certification Support

The Contractor shall ensure ACAS maintains interoperability certification by the Joint Interoperability Test Command (JITC) in accordance with Chairman Joint Chiefs of Staff (CJCS) Instruction 5123.01H. All documentation delivered also shall meet recommendations and guidelines defined in DOD Instruction 8330.01. The Contractor shall comply with the most current version of each reference. The Contractor shall review and provide inputs (if applicable) to the ACAS DODAF artifacts provided by the AMC or USTRANSCOM enterprise architecture team and review the Enhanced Information Support Plan (e-ISP).

In support of this effort, the Contractor shall:

- Prepare a Master Test Plan (MTP) and a test procedure for each test event to support JITC certification.
- Validate entrance and exit criteria for each test to include pass/fail criteria for each requirement.
- Collaborate with developers / engineers to construct test descriptions/cases to ensure each test description/case validates the criteria.
- Create test scenarios.
- Provide and maintain schedules to perform testing, and incorporate into the IMS.
- Perform Test Readiness Reviews.

The Contractor shall perform interoperability testing to determine if discrete systems are functioning properly when connected together and ensure the system effectively exchanges information with other participants in a Net-Centric environment. JITC will conduct an interoperability evaluation, and provide a system interoperability test certification based on an analysis of test data collected during operational use of the system. Generally, the Interoperability Test Certification process comprises four basic steps. Joint interoperability testing and evaluation can be a repetitive process as conditions change. The four basic steps are:

Identify (Interoperability) Requirements
Develop Certification Approach (Planning)
Perform Interoperability Evaluation
Report Certifications and Statuses

As a result of performing this task, the contractor shall provide a MTP and test procedures, test scenarios, and test schedule.

4.12. Cloud Platform/Infrastructure Support

The Contractor shall provide System Administration (SA), Database Administration (DBA), and Network Administration supporting ACAS in the CCE focusing on architecting, deploying, maintaining and documenting ACAS infrastructure in the cloud environment. This includes the following activities: supporting the ACAS infrastructure, promoting software deployments, security patching, incident and problem management, monitoring resource usage, application performance,

and managing all system accounts. The contractor shall ensure personnel performing theses duties maintain a current Secret Clearance, with a current T-3 background investigation, and have relevant industry standard certifications in addition to the mandated DoD 8570.01 Information Assurance Workforce Improvement Program Information Assurance Technical (IAT) Level II certification.

5. Task Area 5: Risk Management and Cybersecurity Support

5.1 Risk Management Framework (RMF) Support

The Contractor shall perform tasks including, but not limited to responsibility for developing and maintaining System Security Assessment and Authorization documentation for RMF security authorization. The Contractor shall develop documentation in accordance with (IAW) DOD Instructions (DODI) 8500.01 Cybersecurity, DODI 8510.01 Risk Management Framework (RMF) for DOD Information Technology (IT), and National Institute of Standards and Technology (NIST) Special Publication(SP) SP 800-39 Managing Information Security Risk, NIST SP 800-53 Information Assurance Controls and Enhancements, NIST SP 800-37 Risk Management Framework, NIST SP 800-137 Continuous Monitoring, NIST SP 800-30 Risk Assessment, and NIST SP 800-53A Assessment Procedure Development Guidance. In addition, the Contractor shall develop and maintain necessary system security documentation to facilitate security authorization in accordance with DOD Risk Management Framework (RMF).

The contractor personnel must perform RMF and applicable security controls, and Defense Information Systems Agency (DISA) Security Requirement Guides (SRGs) and Security Technical Implementation Guide (STIGs) requirements, NIST SP 800 series (Computer Security), and NIST SP 1800 series (NIST Cybersecurity Practice Guides). The contractor shall ensure that personnel performing this duty maintain a current Secret Clearance, with a current T-3 background investigation, and meet mandated DoD 8570.01 Information Assurance Workforce Improvement Program Information Assurance Management (IAM) Level II certification.

The contractor shall notify the PM after the contractor is aware ACAS is not in compliance with RMF and applicable security control. The contractor shall provide a quick-fix recommendation for each RMF or security control non-compliance. The contractor shall provide a POA&M to the ACAS PM to correct the non-compliance. The contractor shall maintain and update the POA&M until ACAS is complaint with the RMF and applicable security control.

The contractor shall collaborate with the Government's designated Information System Security Manager, currently designated as 375th CSPTS/SCMM, to support ACAS Certification & Accreditation, Authority to Operate, Authorization to Connect, security review efforts, Minor Modification Checklist, and Interim Authority to Test.

The Contractor shall reference the Security Plan as the overarching reference document for security control requirements. The Security Plan shall address all of the applicable DoDI 8510.1 security controls, and shall be recognized as the official system security policy.

Along with the System Security Plan (SSP), the Contractor shall submit a plan and timeline to create any missing cybersecurity supporting artifacts or compelling evidence why a cybersecurity control or artifact is not needed, or does not apply to ACAS. The contractor shall participate in ACAS assess

and authorize activities. The contractor shall develop, manage, and update system security documentation to facilitate ACAS security authorization IAW RMF procedures. The Contractor shall perform security certification activities as required to maintain current authorization and support follow-on authorizations.

The Contractor shall evaluate and determine the impact of changes to the system and environment to ensure security. The Contractor shall assess Government-selected controls annually, perform needed remediation as requested and reported by Government security evaluations and tests, review and update the Security Plan, SAR, and POA&M, and report security status to PM as requested.

The Contractor shall update and maintain the Security Plan to support DoD IA RMF authorization decisions. Annually, the Contractor shall review, update, and certify the system security documentation listed below and included as appendices to the Security Plan. When the Contractor review is completed, the Contractor shall update the title page and change log within each of the artifacts listed below.

- Audit Design Artifact
- Cryptographic Subsystem Artifact
- IA Acquisition Artifact
- Identification and Authentication Subsystem Artifact
- Incident Response Plan Artifact
- Interconnections Artifacts
- Personnel Security Artifact
- Remote Access Artifact Security
- Security Design Document Artifact.
- Security Test Plan Artifact.
- Vulnerability Management Plan Artifact
- Security Classification Guide
- Application System Security Plan
- Risk Management Review Report
- IR Report Form/Log
- Developer's Guide
- List of Interface Design Description Documents
- Software List
- VC06 Report
- ESP CM Plan
- Hardware List
- Functional Architecture
- System Architecture

The government will be responsible for providing policy requirements associated with the program, while the contractor shall be responsible for building and incorporating the language into the required artifacts.

The contractor shall establish an Information Assurance Program to implement and sustain appropriate Information Assurance management, operational, and technical controls and processes required to safeguard DOD non-public information resident on or transiting the contractor's

unclassified information systems from unauthorized access and disclosure. Protection measures applied must be commensurate with the risks (i.e. consequences and their probability) of loss, misuse, unauthorized access, or modification of information. The contractor shall submit for Government approval an overarching security plan that describes their strategy for implementation of Information Assurance and Industrial Security requirements throughout the life of the contract. The security plan shall address the security controls described in National Institute of Standards and Technology (NIST) Special Publication 800-53 (current version), Recommended Security Controls for Federal Information Systems and Organizations (http://csrc.mist.gov/publications/PubsSPs.html), and should be tailored in scope and depth appropriate to the effort and the specific unclassified DOD information.

The contractor shall ensure that the Information Assurance System Security Engineering is involved during any/all changes to the system and/or system architecture, to include the application of all applicable DISA SRGs and STIGs, and NIST publications. As part of the contractor's change control process, the contractor shall ensure participation by the Contractor's Information Assurance (IA) System Security Engineer to evaluate the impact of each system or application change on security. The contractor shall document the results of this evaluation. All application and system modifications shall be made in compliance with all analogous or interfacing Information Assurance component(s) of the GIG Architecture and shall be designed to make maximum use of the DOD enterprise Information Assurance capabilities and services. The contractor shall ensure that Information Assurance System Security ~~p~~personnel maintain a current Secret Clearance, with a current T-3 background investigation, and have certifications mandated by DoD 8570.01 Information Assurance Workforce Improvement Program Information Assurance Technical (IAT) Level III certification.

As the result of accomplishing this task, the contactor shall provide

- System Security Plan (SSP) & Plan for Cybersecurity Support Artifacts. The Contractor shall develop an SSP IAW DOD Instructions 8500.01 and 8510.01, and National Institute of Standards and Technology (NIST) SP 800-18 and SP 800-53a. The SSP will be a formal document that provides an overview of the security requirements for the system and describes the security controls in place or plans for meeting those requirements. The information gathered in paragraph 1.5.5.1 will be included in the SSP as it becomes available so that ACAS remains continuously up to date.
- Security Documents and Artifacts. The Contract shall develop and maintain all security documentation and artifacts to support to facilitate security authorization in accordance with DOD Risk Management Framework (RMF), Static Code Analysis, the Risk Management Framework (RMF), Defense Information Systems Agency (DISA) DISA Security Technical Implementation Guides (STIGs), DISA Security Requirements Guides (SRGs), DODI 8530.01, DOD 8570.01-M (Information Assurance Workforce Improvement Program), and the DOD Cloud Computing Security Requirements Guide.
- Information Assurance Plan

5.3. Cybersecurity Planning Support

The Contractor shall perform Assessment and Authorization and Risk Management activities to maintain system authorization and support follow-on activities. The Contractor shall ensure compliance by providing documentation of applicable RMF Controls, Assessment Procedures

(APs), and Control Correlation Identifiers (CCIs). This may involve coordination with the Government, and other Government appointed Contractors, such as System Administration, Security Engineer, Information System Security Manager, Information System Security Officer, and Functional Subject Matter Expert teams.

Additionally, the Contractor shall provide the required compelling evidence to demonstrate compliance with the requirements of the APs or CCIs, such as screen shots, audit logs, messages, completed forms, signed letters or other documentation, etc. Acceptable compelling evidence per requirements, APs, and CCIs are documented sufficiently per Government Information System Security Manager (ISSM) approval. After contract award, the Government will provide the Contractor a list of the current controls, APs, and CCIs relevant to the ACAS system. The Contractor shall contribute artifacts to demonstrate compliance with the requirements of the APs or CCIs. Some of the security controls within each control family may be inherited from the hosting environment or a third party provider.

Artifacts may include:

a. Logical Diagram
b. Network Diagram
c. Data Flows (PPS)
d. External Interfaces
e. Type of Data Exchange
f. Firewall Rules
g. Authenticated Scans
h. Protection Mechanism(s)
i. Hardware and Software Inventory Lists
j. Memorandums of Agreement/Understanding (MOA/MOU), Service Level Agreements (SLA), Interface Control Agreement (ICD), Interface Requirement Specifications, Interface Design Descriptions
k. Acceptable Use Policy
l. System Architecture Description
m. Contingency Plan
n. STIG/SRG checklists

6. Task Area 6: Cloud Migration Support (Optional)

The Contractor shall perform tasks, including but not limited to migrating ACAS from its on-site hosting environment into the CCE (or a Government directed Cloud Environment) to utilize cloud computing for the Development, Test, Staging, and Production environments. The CCE is the portion of a Cloud Service Provider (CSP) within the security authorization boundaries of USTRANSCOM. The CCE is currently Amazon Web Services (AWS) GovCloud, but that may change in the future. The CSP for the CCE are pending a future contract award. The Contractor shall utilize USTRANSCOM enterprise capabilities and cloud native services when available. The period of performance for this task shall not exceed twelve (12) months, six months is preferred, per recent AF Cloud 1 Program Office formal App Analysis. The Contractor shall provide pricing for this task for a twelve-month period.

The Contactor shall update relevant standard operating procedures, run books, production

procedures, system documentation, tactics, techniques and procedures, and other Cybersecurity/Information Assurance artifacts to support the DoD Risk Management Framework (RMF) process to achieve Interim Authority to Test (IATT) and/or ATO for Initial operational capability (IOC) of the application.

Enterprise capabilities currently provided within the CCE include: DNS, Microsoft Active Directory, Network Time Protocol (NTP), SMTP, Online Certificate Status Protocol (OCSP), Secure Socket Shell (SSH) File Transfer Protocol (SFTP), Palo Alto Firewall, Splunk, Windows Server Update Services (WSUS), Yellowdog Updater Modified (YUM), Centrify, GEOINT Access and Information Sharing (GEOAxIS), RedLock, GitLab, Jenkins, Chef, Artifactory, Fortify Static Code Analyzer (SCA), Fortify Software Security Center (SSC), SonarQube, Nessus Security Manager, Eclipse, Maven, JIRA/Confluence. Additional enterprise capabilities will be added as (CCE) evolves.

Cloud native services available within the CCE are expected to include: Virtual Private Cloud (VPC), Elastic Compute Cloud (EC2), Elastic Block Store (EBS), Simple Storage Service (S3), Identity and Access Management, Relational Database Service (RDS), Lambda, Simple Workflow Service (SWF), Elastic Load Balancer (ELB), CloudWatch, CloudTrail, DynamoDB, ElastiCache, RedShift, CloudFormation, Config, Trusted Advisor, Simple Notification Services (SNS), and Simple Queuing Services (SQS). The specific cloud services approved at each DOD Cloud Computing Security Requirements Guide (DOD CC SRG) Impact level (IL) is listed in the DOD Provisional Authorization (PA) for that IL. The ACAS operational environments (i.e. Test, Staging, Non-Production, Production) require IL6. However, the development environment has a lower IL (e.g., IL4). The DOD cloud services catalog is located at https://disa.deps.mil/ext/CloudServicesSupport/Pages/Catalog-DOD-Approved-Commercial.aspx.

In accomplishing this task, the contractor shall provide:

- Cloud Architecture
- Application Migration Strategy
- Application Deployment Blueprints
- Infrastructure Deployment Blueprints
- Automated DevSecOps CI/CD Pipeline
- Cloud Migration After Action Report (AAR)

- **Design Cloud Migration Architecture**

The Contractor shall provide a loosely coupled architecture while leveraging native cloud services (e.g., Elastic Load Balancing, Auto Scaling, Relational Database Services, etc.) that can be easily ported to a Cloud Service Provider. The proposed cloud architecture shall include operating system instances, storage, network topology, and Government-specific security controls. The Contractor shall take into consideration a microservices-based architecture, stateless

application, serverless computing, containerization, automated application and infrastructure deployment, automated scaling, high availability, and cost optimization. The Contractor shall ensure the cloud architecture enables software deployments from the Development environment through the Production environment. The Contractor shall document scaling procedures for operational scenarios that would necessitate a change in compute or storage for up to 30 concurrent users. The Contractor shall develop the proposed cloud architecture in coordination with the appointed Government Technical Subject Matter Experts to attain final Government approval. The Contractors shall provide an highly qualified expert Cloud Architect with extensive demonstrated hand-on experience and relevant industry certifications (e.g., AWS certified Solutions Architect Professional, AWS certified DevOps Engineer Professional, AWS certified SysOps Administrator, AWS certified Advanced Networking), and have expert knowledge and remain current with the Enclave Test and Development STIG, DOD Cloud Computing Security Requirements Guide (SRG), DOD Secure Cloud Computing Architecture (SCCA) Functional Requirements. The Contractor shall ensure that Cloud Architect and Engineer personnel have relevant industry standard certifications in addition to maintain a current Secret Clearance, with a current T-3 background investigation, and the mandated DoD 8570.01 Information Assurance Workforce Improvement Program Information Assurance System Architect and Engineer (IASAE) Level III certification.

The Contractor's Information Assurance System Security Lead shall participate in this activity. The Contractor shall ensure that IA System Security Engineer personnel have relevant industry standard certifications in addition to maintain a current Secret Clearance, with a current T-3 background investigation, and the mandated DoD 8570.01 Information Assurance Workforce Improvement Program Information Assurance Technical (IAT) Level III certification.

- **Develop Application Migration Strategy**

The Contractor shall develop a detailed application migration strategy, which will include the target environment, migration approach, data migration plan, resource plans from both the Government and Contractor, timelines, dependency diagram, risks/issues, estimated costs, test strategies, and Government-specific security controls. The Contractor shall ensure the migration plan identifies and remediates gaps or discrepancies between the current and end state environment, if applicable. The Contractor shall develop the application migration strategy in coordination with the appointed Government Technical Subject Matter Experts to attain final Government approval.

The Contractor shall create an "End State" architecture to fit the application by working with the Government to perform a detailed design of the end-state, cloud-based application and integration architecture, incorporating Government-wide and Government-specific security controls into the target design and migration plan.

The Contractor shall develop and maintain an application migration schedule that defines the timeline, tasks, dependencies, and resources. The Contractor and Government shall ensure this includes all tasks (Government and non-Government) that are required for migration.

The Contractor shall define post-migration test activities (e.g., unit testing, functional testing, performance testing, security testing, failover testing, interface testing with all partners, etc.).

As the result of accomplishing this task, the contractor shall provide:

- Migration Plan:
    - Migration scope, strategy, plan, and schedule
    - Proposed application cloud architecture

Furthermore, the Contractor shall perform any necessary refactoring so the application works effectively and efficiently in the cloud. The Contractor shall consider microservices and service-oriented architecture, stateless application, serverless computing, containerization, automated application and infrastructure deployment, automated scaling, high availability, the number of running instances to allow dynamic scaling, and dynamic-cloud capabilities.

As a result of accomplishing this task, the contractor shall provide a refactored application that meets Government requirements.

- **Build Cloud Enclave Environments**

The Contractor shall adopt the operating procedures and DevSecOps tool chain managed and maintained by the Government to sustain, support, and operate ACAS in the CCE . The Contractor shall build the development, non-production, and production environments in the CCE and validate compliance with applicable STIG/SRG checklists, to include, Enclave Test and Development STIG, DOD Cloud Computing Security Requirements Guide (SRG), DOD Secure Cloud Computing Architecture (SCCA) Functional Requirements. Support the update of relevant standard operating procedures, run books, production procedures, system documentation, tactics, techniques and procedures, and other Cybersecurity/Information Assurance artifacts to support the DoD Risk Management Framework (RMF) process to achieve IATT and/or ATO for Initial operational capability (IOC) of the application.

The Contactor shall provide highly qualified expert cloud architect(s) with extensive demonstrated hand-on experience designing and implementing cloud enclave environments, DevSecOps CI/CD pipelines, and have expert knowledge and remain current with the Enclave Test and Development STIG, DOD Cloud Computing Security Requirements Guide (SRG), DOD Secure Cloud Computing Architecture (SCCA) Functional Requirements. The Contractor shall ensure the Cloud Architect personnel have relevant industry standard certification (e.g., AWS certified Solutions Architect Professional, AWS certified DevOps Engineer Professional, AWS certified SysOps Administrator, AWS certified Advanced Networking). The Contractor shall ensure that Cloud Architect and Engineer personnel maintain a current Secret Clearance, with a current T-3 background investigation, and the mandated DoD 8570.01 Information Assurance Workforce Improvement Program Information Assurance Technical (IAT) Level III certification. The Contractor's Information Assurance (IA) System Security Engineer shall participate in this activity. The Contractor shall ensure that IA System Security Engineer personnel have relevant industry standard certifications in addition to maintain a current Secret Clearance, with a current T-3 background investigation, and the mandated DoD 8570.01 Information Assurance Workforce Improvement Program Information Assurance Technical (IAT) Level III certification.

6..1. Cloud and Build Development Environment

The Contractor shall download the applicable SDKs and become familiar with the CCE , services, procedures, and technologies. The Contractor shall establish, configure, and/or validate a development environment for the application within the CCE to ensure the environment can support development activities (i.e. Develop, Build, Deploy, Test). The Contractor shall establish reusable application and infrastructure deployment blueprints and automated DevSecOps CI/CD pipelines to build, deploy, and test the application from the development environment through the production environment. Templates and/or examples will be provided as they become available to ensure standardization across the CCE environment. Until the CCE is fully operational, the Contractor shall perform operation and maintenance of an on-premise development environment, based on overall Government timelines and CCE operational capability.

As the result of accomplish this task, the contractor shall provide:

- A fully functioning and reusable/promotable Blueprints, cookbooks, and DevSecOps pipeline to support CI/CD
- A validated fully functional Development Environment

6..2. Build Non-Production Environment

The Contractor shall establish, configure, and validate non-production (i.e. Test and Staging) environments using reusable application and infrastructure deployment blueprints and automated DevSecOps CI/CD pipeline to the fullest extent possible to ensure application code changes and infrastructure code changes can be securely promoted from the development environment to support testing activities. This applies to any/all non-production or production environments. During initial states of Cloud environment operationalization, there may be legacy and Cloud environments operating in parallel, to the minimum extent possible.

As the result of accomplish this task, the contractor shall provide:

- A fully functioning and reusable/promotable Blueprints, cookbooks, and DevSecOps pipeline to support CI/CD
- A validated fully functional Test Environment
- A validated fully functional Staging Environment
- End-State system architecture document

6..3. Build Production Environment

The Contractor shall establish and validate a production environment using reusable application and infrastructure blueprints and automated DevSecOps CI/CD pipeline to ensure application code changes and infrastructure code changes can be securely promoted from a non-production environment to support system functionalities, operational data, and business processes.

As the result of accomplish this task, the contractor shall provide:

- A fully functioning and reusable/promotable Blueprints, cookbooks, and DevSecOps pipeline to support CI/CD
- A validated fully functional Production Environment

- End-State system architecture document
- An Operations Manual

- **Automation Support**

The Contractor shall utilize all available orchestration and automation tools for monitoring and performance management, patching, security scans, application deployment, and testing (e.g. unit testing, functional testing, performance testing, security testing, failover testing, interface testing, etc.).

As the result of accomplish this task, the contractor shall provide:

- A fully functioning and reusable/promotable Blueprints, cookbooks, and DevSecOps pipeline to support CI/CD
- Application Deployment Blueprints
- Infrastructure Deployment Blueprints
- Automated DevSecOps CI/CD Pipeline
- Test Scripts
- Test Reports
- Scan Results

- **Cybersecurity of Development, Non-Production, and Production Environments**

The Contractor shall support the RMF process to achieve IATT and ATO for Initial Operational Capability (IOC) of the built development, non-production, and production enclave cloud environments, and the application.

The Contractor shall:

- STIG Compliance: Validate and provide STIG/SRG checklists for the application, supporting application technology stack (i.e., Operating System (OS), Database (DB), Application Server, Web Server, and Runtime), Enclave Test and Development STIG, and DOD Cloud Computing Security Requirements Guide (SRG).
  - Remediate non-compliant checklist items within 21 calendar days.
  - For non-compliant checklist items that cannot be remediated within 21 calendar days, mitigate and submit POA&M items to Authorization Official (AO) for approval.
- Vulnerability Management: Apply security patches to the application technology stack.
  - Installation of security patches for the OS, Database (DB), Application Server, Web Server,etc.
  - For vulnerabilities that cannot be remediated within 21 days, mitigate and submit POA&M items to Authorization Official (AO) for approval.
- Static Code Analysis: Ensure the application does not contain any of the following: new STIG severity Category (CAT) I or CAT II findings, new software errors listed in the current version of the SANS/CWE Top 25 list (http://www.sans.org/top25-software-errors), or new web application security flaws listed in the current version of the OWASP Top Ten list

(https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project).
  - Submit current Fortify scan results with all findings assessed, addressed, and documented in the results files.

- Risk Management Framework (RMF): Update artifacts in the RMF package based on new system architecture, revised application architecture, DevOps culture, and USTRANSCOM CSP environment.
  - Ensure system performance and security posture in CCE environments is equal to or better than on-premises. Performance is measured via user experiences during UAT and in production. Security posture is measured via vulnerability scans, STIG checklists, Static Code Analysis, and risk level in the RMF authorization package.

As the result of accomplish this task, the contractor shall provide:
- Updated RMF System Security Plan (SSP) with appendices
- Completed and validated STIG/SRG checklists (i.e., Operating System, Application Server, Database Server, Web Server, Runtime, Application Security and Development)
- Application Code Scan Analysis Report/Results
- POA&M for non-compliant STIG/SRG checks, non-compliant security patches, and non-compliant Fortify findings
- Security Documents and Artifacts to facilitate security authorization in accordance with DOD Risk Management Framework (RMF) and achieve IATT and ATO.

- **Cutover Support**

The Contractor shall provide cutover support to include testing, and moving the application from its current on-site hosting environment to the CCE.

The Contractor shall perform an Operational Readiness Review (ORR) to determine the application readiness to migrate the application readiness to migrate to the CCE. This shall consist of a review of standard operating procedures including plans, schedules, scripts, and testing/validation in preparation for UAT. The Contractor shall prepare the production CCE for testing and validation for operational suitability. The Contractor shall migrate operational data from on-site database into the CCE. The Contractor shall perform testing to ensure all KPPs and KSAs are met, to include, load testing to ensure usability for 30 concurrent users. The ORR briefing slides shall be delivered one (1) day prior to the ORR.

Contractor shall provide UAT support for functional validation of operational suitability. Failover testing shall be included as part of UAT. The Contractor shall document the results of the UAT within the Government ALM tool; and shall identify, track, and remediate deficiencies from the UAT prior to Government acceptance.

Based on successful completion of UAT, the Contractor shall perform a Production Readiness Review (PRR) that validates the requirements, resolution of all deficiencies from UAT and that the functionality is ready for cutover to the CCE . The PRR slides shall be delivered one (1) day prior to the PRR.

After Government acceptance, the Contractor shall cutover the production environment to the CCE. The Contractor shall maintain support for the on-site system for forty-five (45) business days then decommission once the Government validates it is no longer needed. The Contractor shall support dual operations (CCE and on-site) and resolution of any issues encountered until such time the on-site instance is shut off.

As the result of accomplish this task, the contractor shall provide:

- ORR Briefing Slides
- Test Reports
- Triage Analysis and COAs
- PRR Briefing Slides
- Software Product Specification (Source Code)
- Successful operational data migration to CCE
- Successful operations in CCE
- On-premises support

- **Lessons Learned**

The Contractor shall provide an After Action Report (AAR) on the cloud migration, which captures lessons learned, a summary of the migration actions, and recommendations and considerations related to the cloud migration effort.

As the result of accomplish this task, the contractor shall provide a Migration After Action Report (AAR)

7. Delivery Schedule

Table 2 Contract Deliverables is the authoritative source for the periodicity of all deliverables. The Contractor shall deliver data and software with applicable data rights with the appropriate markings IAW Federal Acquisition Regulation (FAR) 52.227-1, 52.227-2, 52.227-3, 52.227-10, 52.227-11, and Defense Federal Acquisition Regulation Supplement (DFARS) 252.227-7013, 252.227-7014, 252.227-7016, 252.227-7019, 252.227-7025, 252.227-7026, 252.227-7027, 252.227-7030, 252.227-7037, 252.227-7039, and 252.246-7001. The Government obtains under this contract "unlimited rights" to all computer software, software source code, computer software documentation, enhancements, technical data, and similar data developed exclusively at Government expense and delivered to the Government under this contract. "Unlimited rights" means rights to use, modify, reproduce, release, perform, display or disclose in whole or in part, in any manner and for any purpose whatsoever, and to have or authorize others to do so. For all non-commercial software provided by contractor, contractor shall ensure that any individual who creates any of the computer software provides an assignment of any and all proprietary rights in the computer software including all copyrights and patent rights to the software so that the Government has the unlimited rights to the software specified above. It is the contractor's obligation to ensure compliance with all open-source covenants or requirements if any opensource software is included in any deliverable. The contractor shall not use open-source software with licenses that are incompatible with Federal

law and regulation. See Table 2 Contract Deliverables.

The Contractor shall embed the following Code Header in all software components delivered to the Government:

```
////////////////////////////////////////////////////////////////////////////
/// SECURITY CLASSIFICATION: UNCLASSIFIED
////////////////////////////////////////////////////////////////////////////
/// UNLIMITED RIGHTS
/// DFARS Clause reference: 252.227-7013 (a)(16) and 252.227-7014 (a)(16)
/// Unlimited Rights. The Government has the right to use, modify, reproduce, release, perform,
/// display or disclose this (technical data or computer software) in whole or in part, in
/// any manner, and for any purpose whatsoever, and to have or authorize others to do so.
///
/// Distribution Statement D. Distribution authorized to the Department of Defense and
/// U.S. DoD contractors only in support of US DoD efforts. Other requests shall be
/// referred to the Program Executive Officer, USTRANSCOM.
///
///All documents created and delivered under this contract shall be the property of the Government,
///with all intellectual property rights.
///
/// Warning: This document contains data whose export is restricted by the Arms Export
/// Control Act (Title 22, U.S.C., Section 2751, et seq.) as amended, or the Export Administration
/// Act (Title 50, U.S.C., Section 4601 et seq.), as amended. Violations of these export laws
/// are subject to severe criminal and civil penalties. Disseminate in accordance with
/// provisions of DoD Directive 5230.25, Incorporating Change 2, October 15, 2018 and
// DoDI 5230.24, Incorporating Change 3, October 15, 2018.
```

The Contractor shall protect non-public information from unauthorized disclosure IAW DoDI 8582.01, Security of Non-DoD Information Systems Processing Unclassified Nonpublic DoD Information; DODI 5200.48_DAFI 16-1403, Controlled Unclassified Information (CUI); and DFARS 252.204- 7012, Safeguarding Covered Defense Information and Cyber Incident Reporting. For specific CUI (https://www.archives.gov/cui/registry/category-list), see the CUI Registry. The Contractor shall reference The CUI-Marking Handbook.pdf and Protecting DOD's Unclassified Information.pdf (included in GFI.) The contractor shall also comply with the Standards for Privacy of Individually Identifiable Health Information privacy rule issued under the Health Insurance Portability and Accountability Act (HIPAA) of 1996.

All documents created and delivered under this contract shall be the property of the Government, with all intellectual property rights.

Table 2: Contract Deliverables

CDRLs will be post upon official solicitation for subject RFQ

8. Performance Standards

- **Service Delivery Summary**

The Services Delivery Summary (SDS) represents the most important contract objective that, when met, will ensure contract performance is satisfactory. Although not all PWS requirements are listed in the SDS, the Contractor is expected to fully comply with all requirements in the PWS.

The Services Summary table summarizes the most important performance objectives and performance thresholds (specific standards) as identified within the body of the PWS. The absence of any performance objective and threshold from this SS shall not detract from its enforceability nor limit the rights or remedies of the Government under any provision of the contract. The Government Program Manager/COR shall evaluate the contractor on each SS performance objective on a monthly basis and provide a copy of the evaluation to the CO.

Table 3: Services Delivery Summary

Performance Objective	PWS Para	Performance Threshold
All CDRL documentation information provided is accurate, clear, complete, consistent, and contains the appropriate level of detail. All documentation meets professional standards for technical writing and the requirements set forth in the contract. All deliverables clearly identify assumptions and opinions with factual information and/or white papers.	1, 1.1, 1.2, 1.4, 1.5, 2, 3, 3.1, 3.2, 3.5, 3.8, 3.10, 3.23, 4, 4.2-6, 4.9, 4.11, 4.12, 5.1-3, 6, 6.1-7, 7, 8.3, 9, 10.20, 11.1.2-4	No more than 6 documents, per contract period, are returned for rewrites resulting from a) inaccurate, incomplete, or unsupported information; or b) assumptions and opinions not clearly identified and or supported by factual information/white papers. Rewrites are due NLT 5 working days after returned to contractor. Documents containing less than 5 instances of inaccurate, incomplete or unsupported information will not be counted as a rewrite. These documents still need to be updated with correct information and made available to the government. Multiple instances of an error in a document caused by repetitive editing actions (copy/paste) will only be counted as a single error in that document. A document is returned no more than once for correction resulting from a) inaccurate, incomplete, or unsupported information; or b) assumptions and opinions not clearly identified.
All CDRL deliverables are produced using prescribed formats, software tools, and software versions as agreed to by the ACAS PM. Data deliverables are delivered to the Government by the agreed to schedule or in accordance with the terms of the contract	1, 1.1, 1.2, 1.4, 1.5, 2, 3, 3.1, 3.2, 3.5, 3.8, 3.10, 3.23, 4, 4.2-6, 4.9, 4.11, 4.12, 5.1-3, 6, 6.1-7, 7, 8.3, 9, 10.20, 11.1.2-4	No more than one late deliverable per contract period. No late delivery of software releases, unless direct ed by the PM.

Initial responses to the PMO requests for data, information, status are provided within required timeframes	1, 1.1-6, 2, 4.2, 4.4, 4.9, 5.1, 10.19.2, 11.2.14	No instances of late initial responses.
Formal and verbal notice to the PMO of actual or potential problems is reported within required timeframes	1.2, 3, 3.3, 3.5.1, 3.11, 3.22, 4.2, 4.3, 4.4, 4.5, 4.6, 4.9, 5.1, 11.1	No instances of late notices (formal or informal); notifications shale be provided commensurate with problem, i.e. Emergency fix/CAT 1 should be immediately after issue is discovered, etc..
Development environment is maintained in accordance with DISA SRGs and STIGs. Security patches, TASKORDs, MTOs, and Time Critical Network Orders (TCNOs) are maintained to the Government operational environment baseline. Development environment matches the operational baseline (hardware and software), compliance deviation must have prior PM approval	3, 3.17, 3.22, 5.3, 6.3.1, 6.3.2, 6.5	No instance where development environment is not maintained in accordance with DISA SRGs and STIGs. No instances were security patches, TASKORDS, MTOs, and TCNOs are not maintained to the Government operational environment baseline. No instances where development environment does not match the operation baseline (hardware and software), with no compliance deviation without prior PM approval
All delivered software conforms to the requirements in the Version Release List. All delivered software maintains existing functionality, while providing modified capabilities, or systems corrections	2, 3, 3.5, 3.14, 4.3, 6.6	No instances where software release content does not adhere to the Version Release List. No more than one instance, per contract period, where software fails to pass Government acceptance testing. No instances where software does not correctly implement the modified capabilities or system corrections
Interfaces are developed and supported to maintain compatibility among systems in the operational and test environments	3, 3.3, 3.8 3.19, 3.23, 4, 4.3, 4.4, 6.2, 6.4	Satisfactory software performance ratings are achieved during software testing

Level of expertise, coordination, and support necessary to accomplish the contract in a responsive, satisfactory, and timely manner is provided.	1.1, 3, 3.2, 3.3, 3.4, 3.10, 4.7, 4.8, 10.7, App. F	No more than one formal complaint in performance of required tasks. No complaints left unresolved one business day beyond the agreed-to time period.
Testing and evaluation of delivered software releases will adhere to overall testing timeline, to include supporting reviews, i.e. security and configuration management	3.11, 3.22, 4.11, 5.1	Testing/evaluation process will flow, uninterrupted, and found issues are resolved as noted in evaluation process; PM may grant return/redelivery, but timeline shale not be extended
Operational maintenance actions/remediation, to include trouble tickets and operational/security fixes, regardless of size of effort	1.1, 3.5.1, 3.8, 3.12, 3.13, 4, 4.2, 4.3, 4.4, 4.5, 4.7, 4.10, 8.4	Operational sustainment actions will be executed precisely as required, unless PM grants an exception; remediation actions will be accomplished in timely manner as agreed to by PM

Note: The Government reserves the right to inspect or test services that have been tendered for acceptance. The Government shall require performance of any nonconforming services at no increase in contract price. If subsequent performance does not correct the performance issue or correction is not possible, the Government shall seek an equitable price reduction or adequate consideration for acceptance of nonconforming services. The Government will inspect contractor performance IAW the Quality Assurance Surveillance Plan and any other clauses included in the contract. Past performance shall be reported in Contractor Performance Assessment Reporting System (CPARS) to reflect satisfactory or unsatisfactory performance

- **Net Ready – Key Performance Parameters (NR-KPP)**

The Contractor shall ensure ACAS meets all performance parameters and technical requirements identified in the current requirements specifications. The performance of each parameter shall be reported in the MSR. The system shall meet the NR-KPPs identified below.

- **Availability**

The ability for users to sign on and access ACAS is paramount to the success of the program and this will be monitored by measuring the system's ability to allow users to sign on and access the different ACAS environments.

Availability is measured monthly by dividing the time (minutes) that the system was available by the total minutes within the month. This will include scheduled downtime.

An example:

The month of September consists of 43,200 minutes
The system was down 435 minutes in September, so the system was available 42,765 minutes
- 42,765 divided by 43,200 equals .9899
Convert .9899 to a percentage format
Availability = 98.99%
ACAS Availability expectations by environment:
ACAS Production Availability = 99%

The government will supply the format for the reporting that also details system and component degradation. Degradation may not directly affect availability, but it is an important indicator for the PEO for tracking performance trends. An important aspect of Availability reporting is to detail the items that affect availability, or might affect it in the future. The Contractor shall report on what is being done to mitigate these issues.

- **Production Support**

The Contractor shall respond to and resolve operational problems with the system. This task includes responding to incidents, analyzing and correcting specific incidents, creating software development artifacts for systemic problems requiring code changes, and following escalated tickets to resolution. Typical incidents to be resolved under this task include database updates for specific records with incorrect data, which involves determining the cause of the issue, correcting the database, and determining whether a code fix is necessary. Failover and recovery times are described in Table 4:

Table 4: Failover and Recovery Times

	Time to Full Recovery	Downtime allowed
Application failure	15 to 20 minutes	Max. 20 minutes
Database failure	1 hour	Max. 1 hour
Availability zone failure (very rare)	1 hour	Max. 1 hour
Patch maintenance	15 to 20 minutes	None

9. Government Furnished Property (GFP) and Government Furnished Information (GFI), Equipment and applicable software licenses for use within the performance of this contract shall be managed IAW FAR 52.245-1. Examples (but should not be expected, or solely inclusive) include Government provided laptops and software licenses.

The contractor shall provide Information Technology Equipment Custodian (ITEC) services, as defined in Air Force Manual (AFMAN) 17-1203, Information Technology Asset Management (ITAM). All ACAS program equipment and software provided by the Government, to include Government Furnished Equipment (GFE), Government Furnished Software (GFS), and Government

incidental equipment and property, shall be maintained, inventoried, and accounted for by the contractor's ITEC. The Contractor's ITEC shall comply with the tracking requirements of the program CM. The Contractor shall comply with all instructions and regulations provided by the Scott Air Force Base Equipment Management office (375 CS/SCBCE), or its successor organization, and the Base Equipment Control Office (BECO). The Government will provide the contractor with access to DOD and Air Force publications, directives, policy letters and standards relevant to ITEC responsibilities. The Contractor shall verify all equipment is accurately listed in the Information Technology Asset Management system, or its successor system, and work closely with the ACAS PM and the BECO. The Contractor shall provide an Asset Management Report (AMR) to the ACAS PM and/or COR monthly. The AMR shall be a complete list of GFE and GFS currently in the Contractor's possession and accountable under this effort, as applicable.

- **Government Furnished Equipment (Computers)**

The Contractor shall utilize Government furnished computers to perform all tasks. The use of privately owned computers (i.e. computers not owned and provided by the Government) to process classified information is prohibited. Neither personally owned hardware nor software will be used in the official performance of Government business nor will it be installed on Government information assets for personal use or gain. Additionally, use of entertainment and games software is prohibited.

- **Government Furnished Software (GFS)**

The Contractor shall utilize Government furnished software to perform tasks. The use of privately owned software (i.e. software not owned and provided by the Government) in the Software Development Life Cycle is prohibited. Neither personally owned software will be used in the official performance of Government business nor will it be installed on Government information assets for personal use or gain. Additionally, use of entertainment and games software is prohibited.

- **Government Furnished Information (GFI)**

The Contractor shall consider the GFI list in Appendix A for fulfillment of contract requirements.

- **Government Asset Management Report (AMR)**

The contractor shall prepare and maintain an AMR.

The contractor shall provide initial inventory within five workdays after contract award to COR and report to the COR via marked-up inventory report any discrepancies between the list of Government property provided and the actual inventory.

a. The contractor shall update the AMR every 30 calendar days after completion of the initial inventory.

b. The contractor shall provide to the Government a fully reconciled AMR NLT 28 February of each year with the final AMR due NLT five days prior to contract completion.

The contractor shall provide the final AMR consisting of an unalterable Government verified inventory and a duplicate inventory recorded in Excel that may be altered by the Government.

- **Secret Internet Protocol Router Network (SIPRNET)**

The Contractor must have access to SIPRNET to fulfill this requirement. This access will be used for tasks such as viewing Information Assurance and security notifications, Cyber Hygiene Scorecard, and participating in Classified Defense Collaboration Services meetings to illustrate bugs/features. If the Contractor does not have SIPR access, the Government will facilitate coordination with the Base for the Contractor to meet this requirement. It shall be the Contractor's responsibility to meet all the requirements and provide all required documentation to the local facility. The Government will not pay for SIPR access at the Contractor's facility. The Government will issue CACs and SIPRNET tokens to Contractor employees.

10. General Information

- **Place of Performance**

Tasks shall be performed at the Contractor's facility. On occasion, Contractors who work at the Contractor facilities will be required to attend meetings at AMC or USTRANSCOM, Scott AFB, IL. The Government will provide up to four controlled working spaces at Scott AFB primarily for Help Desk support and as needed for SIPR access.

Contractor activities will be performed at Scott AFB, or at a Contractor facility located within local Scott AFB area (25-mile radius). Frequent/daily interface with the customer at Scott AFB is needed for detailed requirement development and prototype demonstrations. Frequent travel between the contractor's facility and Scott AFB IL will be required. All meetings, reviews, and audits will be held at Scott AFB or the local Contractor facilities, except when alternate locations are agreed upon by the Contractor and the COR. Management, technical studies, analysis, and associated activities may be conducted at the most feasible and economical location. Overall, any interfacing events requiring Government attendance, not conducted at Scott AFB, the location of performance will be within a 10-mile radius of Scott AFB. Contractor activities requiring access to the SIPRNET shall be performed at Scott AFB.

10..1. Alternate Place of Performance

As determined by the Contracting Officer's Representative (COR), contractor employees may be required to work at an alternate place of performance (e.g., home, the contractor's facility, or another approved activity) in cases of unforeseen conditions or contingencies. Non-emergency/non-essential contractors should not report to a closed government facility.

10..2. Health and Safety on Government Installations

In performing work under this contract on a Government installation IAW Air Force Federal Acquisition Regulation Supplement (AFFARS) 5323.9001, the contractor shall:

(1) Take all reasonable steps and precautions to prevent accidents and preserve the health and safety of contractor and Government personnel performing or in any way coming in contact with the performance of this contract; and
(2) Take such additional immediate precautions as the contracting officer may reasonably require for health and safety purposes.

The contracting officer may, by written order, direct Air Force Occupational Safety and Health (AFOSH) Standards and/or health/safety standards as may be required in the performance of this

contract and any adjustments resulting from such direction will be in accordance with the Changes clause of this contract.

Any violation of these health and safety rules and requirements, unless promptly corrected as directed by the contracting officer, shall be grounds for termination of this contract in accordance with the Default clause of this contract.

- **Hours of Work**

Contractor employees shall be available to correspond and attend meetings with the Government during normal Government duty hours. The average Government workweek is based on 40 hours. Typical work hours for the Government are between the hours of 0730 and 1630, Monday through Friday Central Standard Time. Contractor personnel providing situational support may be required to support three-shift functions or as specified by the COR. Personnel may be required to support short notice adjustments to the daily work hours. Helpdesk operations are expected 24/7/365.

Certain PWS requirements, like the support of the production environment, dictate additional duty hours to facilitate 24 hours per day, 7 days per week, 365 days per year (24x7x365) support and on call services. The level or extent of work, after normal duty hours when in response to Trouble Tickets received and managed by the Help Desk is comprised solely as triage to determine the level of effort to resolve Tier 2 and Tier 3 level of work. Actual resolution of Trouble Tickets beyond Help Desk capabilities will be resolved as soon as possible, during normal duty hours, when possible. Contractor personnel may also be required to work designated holidays, any other customer observed days designated by: (i) Federal Statute; (ii) Executive Order; or (iii) a Presidential Proclamation to support PWS tasks or as specified by the COR. Government surveillance of Contractor performance is required to give reasonable assurance that efficient methods and effective cost controls are used. The contractor shall ensure continuity of operations during periods of personnel turnover and long-term absences. Long-term absences are those longer than two weeks duration.

- **Account Management**

The Contractor shall provide a list of employee names and positions in order to establish the appropriate account permissions. The Contractor shall notify the COR no later than 24 hours after changes in personnel occur. See paragraph 11.2.7 for Common Access Card (CAC) issuance procedures.

- **Section 508 Accessibility**

All Electronic and Information Technology (EIT), as defined at FAR 2.101, supplied under this contract, must conform to the Architectural and Transportation Barriers Compliance Board Information and Communication Technology (ICT) Accessibility Standards (36 CFR Part 1194). The applicable standards are available at http://www.access-board.gov/sec508/guide/index.htm. The following Section 508 Reference Guides have been determined to be applicable to this contract:

10..1. Technical Standards

- **1194.21 Software applications and operating systems**

- **1194.22 Web-based intranet and internet information and applications**
- **1194.23 Telecommunications products**
- **1194.24 Video and multimedia products**
- **1194.25 Self-contained, closed products**
- **1194.26 Desktop and portable computers**
- **1194.41 Information, Documentation and Support**

The Technical Standards above facilitate the assurance that the maximum technical standards are provided to the Contractors.

10..2. Functional Performance Criteria

Functional Performance Criteria are minimally acceptable standards to ensure Section 508 compliance and acceptable EIT/ICT products are proposed.

- **1194.31 Functional Performance Criteria**

- **Travel**

The contractor will be required to have two individuals travel twice per year to Cambridge, MA for four days to attend technical exchange meetings, if directed by PMO.

Location	Number of Trips per Year	Number of Days per Trip	Number of People per Trip
Cambridge, MA	2	4	2

Trip reporting is due five business days following completion of travel.

- **Period of Performance**
  - Phase-In: 01 January 2024 – 31 January 2024
  - Base Period: 01 February 2024 – 30 September 2024
  - Option Period 1: 01 October 2024 – 30 September 2025
  - Option Period 2: 01 October 2025 – 30 September 2026
  - Option Period 3: 01 October 2026 – 30 September 2027
  - Option Period 4: 01 October 2027 – 30 September 2028
  - Optional Six-Month Extension of Services (EOS): 01 October 2028 – 31 March 2029

- **Specialized Skills Required**

The Contractor, as a whole, must possess the skills and knowledge required to fulfill requirements of this contract. If the Contractor utilizes other sources, outside of primary vendor, to fulfill skill/knowledge requirements, the Contractor must manage and be able to provide the required expertise in a manner same as if from primary vendor, i.e., same time and availability as contract personnel at local work site. Appendix F lists subject skills/knowledge, but not limited solely as listed, as the Contractor must evolve knowledge, as the system evolves.

- **Velocity**

The velocity of the team must be maintained to ensure predictable results. The Government's requirement is for ninety-five percent (95%) of committed artifacts (above the waterline) to be deployed and 95% to be free of defects.

- **Latent Defects**

If a software change results in a latent defect found during operation at a future time, and analysis determines the Contractor's personnel made the errant change, the defect shall be corrected by Contractor personnel without affecting software sprint/release velocity. In short, the Government will not pay for the change twice.

- **Non-Personal Services**

The Government will neither supervise contractor employees nor control the method by which the contractor performs the required tasks. Under no circumstances shall the Government assign tasks to, or prepare work schedules for, individual contractor employees. It shall be the responsibility of the contractor to manage its employees and to guard against any actions that are of the nature of personal services or give the perception of personal services. If the contractor feels that any actions constitute, or are perceived to constitute personal services, it shall be the contractor's responsibility to notify the task order Contracting Officer (CO) immediately. These services shall not be used to perform work of a policy/decision making or management nature, i.e., inherently Governmental functions. All decisions relative to programs supported by the contractor shall be the sole responsibility of the Government.

- **Organizational Conflicts of Interest (OCI)**

If at any time during performance of PWS requirements, the contractor becomes aware of an actual or potential OCI situation or issue, or the appearance of an actual or potential OCI situation or issue exists, the contractor shall identify in writing, to the COR and CO, the nature of the OCI situation or issue, along with a plan to mitigate the OCI situation or issue.

- **Company to Company Nondisclosure Agreements**

During performance of this contract, contractor employees may require access to proprietary information from other Government support contractors. This may result in the contractor gaining an unfair competitive advantage. Therefore, in order to protect the contractors' information and encourage companies to provide it when necessary for contract performance, a contractor that gains access to proprietary information of other companies in performing these services for the Government must agree with the other companies to protect their information from unauthorized use or disclosure for as long as it remains proprietary and refrain from using the information for any purpose other than that for which it was furnished. The contractor shall provide the CO with copies of any such agreements so that the CO can ensure that they are properly executed.

- **Personnel Requirements**

The contractor shall make every effort to retain personnel in order to ensure continuity until Contract completion. If it should become necessary to substitute or replace personnel, the contractor shall immediately notify the COR and CO in writing of any potential vacancies. The contractor shall

inform the Government of what projects or assignments might be affected with a change in personnel. The contractor shall make every reasonable attempt to fill any vacancy of a position described in a time period not longer than a single billing cycle. Contractor employees providing services directly on this contract shall read, write, speak, articulate, and comprehend technical English language to the extent necessary for the performance of the work. The Government has the right of refusal for replacement personnel that do not meet the requirements of the PWS.

- **Key Personnel**

The contractor shall submit the resumes of replacement key personnel selected to perform to the COR and CO for Government review and validation skill sets. The contractor shall identify key personnel in the Technical and Management Work Plan.
The contractor shall provide the name of the contractor Site Manager and contractor Alternate Site Manager Key Personnel in the Technical and Management Work Plan. In the event both the contractor Site Manager and Alternate Site Manager are unavailable for more than one business day, the contractor shall notify the COR of an alternate point of contact (POC). The contractor shall also provide the names of the technical lead experts and one technical lead backup for system administration, network administration, and database administration on the Technical and Management Work Plan. The contractor shall notify the CO and the COR in writing not later than five business days before a vacancy of any of the key personnel identified in Para Section 2.0 of this PWS occurs.

- **Identification of Security and Non-Disclosure Requirements**

The governing security policy documents include DODI 8500.01, DoD 8570.01-Manual (M), Information Assurance Workforce Improvement Program (IAT Level II: https://www.sans.org/dodd-8570/) and CJCSM 6510.01, Information Assurance (IA) and Support to Computer Network Defense (CND), and as defined in Appendix E .
In performance of this contract, the Contractor shall have access to sensitive, non-public information. The contractor agrees (a) to use and protect such information from unauthorized disclosure IAW DoDI 8582.01 Series, Security of Unclassified DOD Information on Non-DOD Information Systems; (b) to use and disclose such information only for the purpose of performing this contract and to not use or disclose such information for any personal or commercial purpose; to obtain permission of the Government before disclosing/discussing such information with a third party; (d) to return and/or electronically purge, upon Government request, any non-public, sensitive information no longer require for contractor performance; and (e) to advise the Government of any unauthorized release of such information. The Government will require contractor personnel to sign a non-disclosure agreement (NDA) to protect non-public information of other contractors and/or the Government. The NDA shall be signed and provided to the Government within one week of contract award. The Contractor shall be responsible for obtaining and maintaining NDAs for each Contractor employee assigned to the contract. Information may only be discussed with those persons outlined on the non-disclosure form. In addition, frequent interactions with other Contractors and contractor proprietary information may be required. The contractor must agree with the other companies to protect their information from unauthorized use or disclosure for as long as it remains proprietary and refrain from using the information for any purpose other than that for which it was furnished. The contractor shall provide copies of those agreements to the contracting officer and ensure that they are properly executed. The execution of said agreements shall be the sole responsibility of the Contractor. The NDA (Appendix D) is located in the references section of the PWS. PMO will

assist contractor when determining categorization of information/data within ACAS, by working with the AMC Information Protection Office (AMC/IP).

- **Quality Assurance**

The Contractor shall support Government agency reviews and audits of all services and support provided under this PWS. The Contractor shall support Quality Assurance reviews conducted by the Government.

The Government reserves the right to authorize an independent verification and validation of the Contractor's procedures, methods, data, equipment, and other services provided during the performance of this PWS.

- **Standards**

ACAS program aligns to the Joint Deployment and Distribution Architecture -Enhanced, which is managed by the USTRANSCOM Chief Architect in the Command, Control, Communications and Cyber Systems Directorate (TCJ6). The Contractor shall abide by the Joint Deployment and Distribution Architecture Enhanced (JDDA-E) standards. Also adhere to references and directives/guidance listed in Appendix A.

- **Requirements Affecting Contractor Personnel Performing Mission Essential Services**

Certain personnel providing services under this Contract will be designated as Mission Essential Personnel. Contractor shall ensure personnel required to accomplish tasks designated as Mission Essential Personnel report to assigned work locations and perform required tasks, regardless of weather or security conditions. The government has identified task areas at 4.2, 4.3, 4.4, 4.5, 4.6, 4.7, 4.8, 4.9 and 4.12 as Mission Essential. The contractor shall provide a Mission Essential Contractor Services Plan with the proposal for evaluation. The contractor shall provide a list of essential personnel required to perform the tasks to CO and COR no later than 10 working days after contract start. This list will be maintained by the contractor with updates provided to the CO and COR with any personnel changes or as required. The CO and/or COR will be responsible for providing government security personnel with list of contractor Mission Essential Personnel to enable access to government facilities when non-essential personnel are barred. Contractor shall operate in accordance with DFARS 252.237-7023 Continuation of Essential Contractor Services. Mission Essential Personnel are personnel allowed to enter Scott AFB during periods of restricted access as designated by the Base Commander.

- **Contract Transition**

Prior to contract expiration, or in the event of a different Contractor winning a follow-on contract, the Contractor shall provide, at a minimum, all materials and support necessary to accomplish a seamless and expeditious transition of the tasks identified in this PWS to the incoming Contractor. The Contractor shall include electronic copies of the following: all in- progress working files, Concept of Operation (CONOPS) procedures, and final phase out meeting with Government, incumbent and the new Contractor. The Contractor shall support a formal contract closeout process, including the documenting of lessons learned throughout the life of the contract. All deliverables shall be provided sixty (60) business days before the end of the contract period of performance.

10..1. Phase-In

Upon contract start, the contractor shall accomplish the following phase-in transition tasks:

- Implement the proposed methods, processes, procedures, and tools necessary to design, modify, and deliver software meeting the requirements provided by the Government as described in the approved Management Plan.
- Assume technical support responsibilities.
- Assume overall software design and modification responsibilities.
- Assume testing responsibilities.
- Assume responsibilities for GFP, to include, GFE and GFS
- Appoint an Equipment Custodian (EC) and assume responsibility for Information Technology (IT) Asset Management (ITAM) ACAS account.
- Move the GFE supporting this task to the Contractor's facility. The Contractor shall be responsibility for transporting the GFE to the Contractor's facility.

Within 45 calendar days after contract start, the contractor shall, in conjunction with a Government representative, conduct a joint inventory of GFP, to include, GFE and GFS, and reconcile with the list provided. From the inventory reconciliation, provide a Government Furnished Property Report (ARM) for all GFP.

10..2. Phase-Out

Contractor shall provide a phase-out plan describing the method of transferring responsibility for tasks described in the PWS. The contractor shall cooperate fully with the Government and any successor contractor(s) to ensure an orderly transition at the end of this contract. Provide recurring status briefings to the Government and associate contractors throughout the transition period.

The contractor shall preserve and make available to the COR, if requested, copies of all records and other documentation, developed or acquired under this contract or preceding contracts for this effort, regarding performance of the work required by this contract.

The contractor shall make available to the COR, upon request, the names, job titles, and duties of all employees who have worked under this contract;

The contractor shall permit current employees to be interviewed for possible employment by a successor contractor;

The contractor shall provide, as requested by the ACAS PM, an orientation for successor contractor employees.

The contractor shall supply to the Government, 60 calendar days prior to the completion of the contract, the following information:

- Complete backup of all contract and contract related data stored on each employee's hard drive, along with any global data.
- A list of all GFP and COTS utilized in support of this task.
- Soft and hard copies of all procedures and materials developed as part of this effort.

The contractor must ensure that no contract data is corrupted, changed, or altered such that it would cause damage to the Government.

Within 60 calendar days of contract completion, the contractor shall, in conjunction with a Government representative, conduct a joint inventory of the GFP, to include, GFE and GFS and reconcile with the AMR.

As the result of accomplishing this task, the contractor shall provide:

- Transition Plan
- In-Progress Working Files
- Concept of Operations (CONOPS) Procedures
- Lessons Learned

- **Contractor Manpower Reporting**

In order to support the requirements of title 10, U.S.C., section 235 and 2330a, DoD contractors will report ALL contractor labor hours (including subcontractor labor hours) required for performance of services provided under this contract for AMC, via the Service Contract Reporting (SCR) section of the System for Award Management (SAM) (http://sam.gov). Reporting inputs will be for the labor executed during the period of performance for each Government fiscal year (FY), which runs 1 October through 30 September. While inputs may be reported any time during the FY, all data shall be reported no later than 31 October of each calendar year. A DoD Guidebook for Service Contract Reporting in the SAM is available at https://dodprocurementtoolbox.com/site-pages/service-contract-reporting-scr. GSA has posted guidance at https://sam.gov, search the "HELP" section. Should contractors have issues using SAM, contact the Federal Service Desk at https://www.fsd.gov.

10.21 Contractor Communications

In order to reduce confusion during meetings or communications, ensure all contract personnel have their company and position identified in all digital and written communications, to include identification during teleconferences. When contract personnel are on Scott AFB, they will adhere to current identification standards by wearing a specific lanyard identifying them as contractors. Contract personnel with CAC identification can access Scott AFB without escort, but will have to obtain specific contract identification from Government sponsor, prior to entering specific Government facilities/meeting locations.

11. Security

- **Cybersecurity for (Non-TSP Contracts– Operationally Critical Support)**

11..1. Operationally Critical Support

The services designated under this contract are "operationally critical support" as defined in DFARS 252.204-7012.

11..2. Cybersecurity Incident Reporting

11..2.1. In addition to the DFARS 252-204-7012 reporting requirements for unclassified systems and DoDM 5220.22, Volume 2_DAFMAN 16-1406, Volume 2, *National Industrial Security Program Operating Manual (NISPOM)* for classified systems, reportable cyber incidents include the following:

11..2.2. Unauthorized data exfiltration, manipulation or disclosure of any DoD information resident on or transiting the contractor's (or its subcontractors') unclassified or classified information systems or networks.

11..2.3. Unauthorized access to the contractor's (or its subcontractors') unclassified or classified information system(s) or networks(s) on which DoD information is resident or transiting.

11..2.4. Cyber incidents as listed in the MITRE ATT&CK Framework available at https://attack.mitre.org/, which is incorporated herein by reference.

11..2.5. Notifications by a federal, state, or local law enforcement agency or cyber center (i.e., National Cyber Investigative Joint Task Force (NCIJTF), National Cybersecurity & Communications Integration Center (NCCIC)) of being a victim of a successful or unsuccessful cyber event, anomaly, incident, insider threat, breach, intrusion, or exfiltration.

11..2.6. If the cyber incident affects a classified system, vulnerabilities associated with the incident will be classified per the current version of USTRANSCOM Instruction 31-02, Security Classification Guide. Additionally, the contractor shall adhere to FAR 52.204-2 and comply with reporting requirements as outlined DoDM 5220.22, Volume 2_DAFMAN 16-1406, Volume 2 (Current version).

11..3. Cybersecurity Incident Reporting Timelines

In addition to providing the notification required by DFARS 252.204-7012, the contractor is required to notify USTRANSCOM and PMO SM and PM as soon as practicable, but no later than 4 hours after discovering a reportable cyber incident. The reporting timeline begins when the incident is discovered or reported to the company, its employees, contractors, or cybersecurity firm responsible for providing cybersecurity and response for the company. The contractor shall contact the USTRANSCOM Cyber Operations Center (CyOC) via phone at 618-220-4222. If the contractor does not immediately reach the CyOC via phone, the contractor shall send an email notification to transcom.scott.tcj6.mbx.cyoc@mail.mil.

11..4. Mandatory Reporting Data

11..4.1. The contractor shall work with the USTRANSCOM CyOC through resolution of the incident. Within 4 hours of becoming aware of a reportable cyber incident, the contractor shall provide an initial notification of the incident, even if some details are not yet available, which includes the following information:

(a) Company Name
(b) Who will be the POC with contact information
(c) Contracting Officer POC (name, telephone, email)
(d) Overall Assessment –Description of incident, data at risk, mitigations applied
(e) Indicators of compromise
(f) Vector of attack (if known)
(g) Estimated time of attack (if known)

11..4.2. The contractor shall provide a follow-on cyber incident report to the USTRANSCOM CyOC within 24 hours of becoming aware of a reportable cyber incident, which includes the following information:

(a) Contractor unique Commercial and Government Entity (CAGE) code
(b) Contract numbers affected
(c) Facility CAGE code where the incident occurred if different than the prime Contractor location
(d) POC if different than the POC recorded in the System for Award Management (name, address, position, telephone, email)
(e) Contracting Officer POC (name, telephone, email)
(f) Contract clearance level
(g) Name of subcontractor and CAGE (if applicable) code if incident occurred on a subcontractor network
(h) DoD programs, platforms, systems, or information involved
(i) Location(s) of compromise
(j) Date incident discovered
(k) Type of compromise (e.g., unauthorized access, inadvertent release, other)
(l) Description of technical information compromised
(m) Any additional information relevant to the information compromise

11..5. Reporting Coordination

11..5.1. In the event of a cyber-incident, USTRANSCOM may conduct follow-on actions that include an on-site review to assist the contractor in evaluating the extent of the incident and to share information in an effort to minimize the impact to both parties. Date and time of on-site visits will be mutually agreed upon by USTRANSCOM and the contractor in advance.

11..5.2. The contractor agrees to allow follow-on actions by the Government (e.g., USTRANSCOM, Federal Bureau of Investigation, Department of Homeland Security,

DC3, etc.) to further characterize and evaluate the suspect activity. The contractor acknowledges that damage assessments might be necessary to ascertain an incident methodology and identify systems compromised as a result of the incident. Once an incident is identified, the contractor agrees to take all reasonable and appropriate steps to preserve any and all evidence, information, data, logs, electronic files and similar type information (reference NIST Special Publication 800- 61: Computer Security Incident Handling Guide, (current version) related to the incident for subsequent forensic analysis so that an accurate and complete damage assessment can be accomplished by the Government.

11..5.3. The contractor is not required to maintain an organic forensic capability, but must ensure data is preserved (e.g., remove an affected system, while still powered on, from the network) and all actions documented until forensic analysis can be performed by the Government or, if the Government is unable to conduct the forensic analysis, a mutually agreed upon third party (e.g., Federally Funded Research and Development Center (FFRDC), commercial security contractor, etc.). Any follow-on actions shall be coordinated with the contractor via the Contracting Officer.

11..5.4. The contractor agrees to indemnify and hold the government harmless for following any recommendations to remedy or mitigate the cyber-incident following the actions under 11.1.5.1 and 11.1.5.2.

11..6. Confidentiality and Non-Attribution Statement

The Government may use and disclose reported information as authorized by law and will only provide attribution information on a need-to-know basis to authorized persons for cyber security and related purposes (e.g., in support of forensic analysis, incident response, compromise or damage assessments, law enforcement, counterintelligence, threat reporting, and trend analysis). The Government may share threat information with other USTRANSCOM industry partners without attributing or identifying the affected contractor.

11..7. Subcontracts.

11..7.1. The contractor shall include the above cyber security language in paragraphs 11.1.1 through 11.1.7 in subcontracts, or similar contractual instruments, including subcontracts for commercial items, without alteration, except to identify the parties.

11..7.2. The contractor shall require subcontractors to report cyber incidents defined in paragraph 11.1.3. to the prime contractor when DoD's information resides on the subcontractor's system(s) or network(s).

- **Physical, Personnel, Information, Antiterrorism/Force Protection and Industrial**

11..1. General Security Information.

The majority of daily work associated with this PWS is at the unclassified level, but contractor personnel may be required to access SECRET information and/or classified areas, during performance of this task order.

11..2. Citizenship and Clearance Requirements

The contractor's, subcontractors, and/or partner's personnel performing services under this task order shall be citizens of the United States of America. Overall, all contractor personnel shall possess the appropriate personnel security investigation for the position(s) occupied. Contractor personnel shall be required to have a background investigation that corresponds with the sensitivity level of the tasks to be performed. Note that neither dual citizens nor non-US citizens are eligible for Common Access Cards (CACs) unless they meet the parameters stated in DoDM 1000.13, volume 1.

11..3. Clearance Requirements and Position Sensitivity

Contractor personnel with IA administrative privileges and/or who will monitor DOD IT systems or software as designated by DOD Instruction 8500.1 and DoDM 5200.02_AFAMN 16-1404 may be rated at the various levels listed below. The stipulation of the numbers and what IT/Automated Data Processing (ADP) levels the contractors will have is approved by the COR or the CO before the start of the task order. The contractor shall comply with all appropriate provisions of applicable security regulations while assigned to this task order for DOD and USTRANSCOM. The following guidance will be followed when determining background investigation and clearance levels for this task order depending on requirements:

POSITION LEVEL:
Information Technology (IT)-II Automated Data Processing (ADP)-II
Or Non-Critical Sensitive Positions (SECRET):
IT/ADP-II and Non-Critical Sensitive Positions are those positions that: have access to Secret or Confidential information; Security police/provost marshal-type duties involving the enforcement of law and security duties involving the protection and safeguarding of DOD personnel and property; category II automated data processing positions; duties involving education and orientation of DOD personnel; duties involving the design, operation, or maintenance of intrusion detection systems deployed to safeguard DOD personnel and property; responsible for the direction, planning, design, operation, or maintenance of a computer system, and whose work is technically reviewed by a higher authority of the ADP-I category to ensure the integrity of the system; and any other position so designated by the head of the Component or designee.

BACKGROUND INVESTIGATION REQUIREMENTS:
(IT-II/ADP-II/Non-Critical Sensitive) Requirements for SECRET – (Tier 3):
Positions designated by the Government at the Non-Critical Sensitive/ADP-II/IT-II rating require a Tier 3 (or acceptable periodic reinvestigation) favorably adjudicated (a favorable adjudication grants eligibility at the SECRET level as prescribed by DoDM 5200.02_AFAMN 16-1404). The IT-II/ADP-II requirement mandates the contractor have a minimum FCL at the SECRET (or higher) level due to investigation submissions as directed in DoDM 5220.22, Volume 2_DAFMAN 16-1406, Volume 2, DoDM 5200.01, Volume 1_DAFMAN 16-1404, Volume 1, DoDM 5200.01, Volume 2_DAFMAN 16-1404, Volume 2, and DoDM 5200.01, Volume 3_DAFMAN 16-1404, Volume 3, and Defense Information Security System (DISS).

POSITION LEVEL:
Information Technology (IT)-III Automated Data Processing (ADP)-III
Or Non-Sensitive Positions (Position of Trust Determination) (No Classified Access–Tier 1) All other positions involved in computer activities and Common Access Card. No clearance is granted

for classified access and only a Position of Trust (PoT) is awarded and posted in DISS.

BACKGROUND INVESTIGATION REQUIREMENTS:

(Non-Sensitive/IT-III/ADP-III) Requirements for Position of Trust Determinations (No Classified Access - Tier 1/NACI):

Positions designated by the Government as Non-Sensitive/IT-III/ADP-III require a favorably adjudicated Tier 1/NACI investigation or greater IAW DoDI 5200.46, DoD Investigative and Adjudicative Guidance for Issuing the Common Access Card (CAC), dated 9 Sep 2014, DoDM 1000.13, Vol 1, DoD Identification (ID) Cards: ID Card Life-Cycle, dated 23 Jan 2014, and National Background Investigations Bureau (NBIB) standards. Before a CAC or NIPRNet access will be granted, a favorable Tier 1/NACI investigation or greater must be on record in DISS, and a favorable Federal Bureau of Investigation (FBI) National Criminal History Check (fingerprint check) on record with the National Background Investigations Bureau (NBIB). A CAC may be issued on an interim basis based on a favorable FBI fingerprint check and successful submission of a Tier 1 investigation to NBIB, and on record in DISS.

NOTE: The above requirements for Non-Sensitive/IT-III/ADP-III positions are for unclassified access and systems only. No classified access will be granted based on the Tier 1 investigation. USTRANSCOM will only process Tier 1 investigations and will not complete any personnel security investigations (Tier 3/Tier 5) for classified access. It is incumbent upon the contractor to have the appropriate investigations completed upon start of the task order.

11..4. Security Clearance and Special Access Requirements

All positions on this task order require a minimum of either an interim SECRET clearance as granted by the Vetting Risk Operations Center (VROC), or a completed adjudication of SECRET clearance granted by the DoD Consolidated Adjudication Facility (CAS).

11..5. Facilities Clearance (FCL)

The contractor must have a valid FCL at the SECRET level. FCL procedures and security guidelines for adjudicative requirements are outlined in DoDM 5220.22, Volume 2_DAFMAN 16-1406, Volume 2. FCLs and interim FCLs must be awarded by the Defense Counterintelligence and Security Agency (DCSA) Facility Clearance Branch.

11..6. Personnel Clearance Validation

Upon contract/task order award, the contactor shall submit the names of contractor personnel to the Government contracting team, who will provide to TCCS-PR for vetting through DISS or the Defense Information Security System (DISS) to ensure investigative and clearance requirements have been satisfied. This shall be completed before the COR/Trusted Agent (TA) accesses the DOD Trusted Associate Sponsorship System (TASS) and submits a request for issuance of the CAC to the contractor's personnel. If a contractor's employee does not have the required investigative or security clearance level based on the Government's determination, the contractor's employee will be denied the ability to work in support of this contract/task order.

11..7. Common Access Card Issuance Procedures

Upon contract or task order award, if any of the United States (U.S.) citizen contractor employee, requires a CAC, the contractor shall submit the names of all such personnel to the Contracting Officer (CO) or Contracting Officer Representative (COR), if they are found qualified in DISS, by the FSO. If the CO or COR determines any of the employees require a CAC, the contract Trusted Associate Sponsorship System (TASS), Trusted Agent (TA), may create a CAC application in

TASS. The TA must submit the names to the TASM for verification of their background investigation, before a CAC is approved.

a) For those personnel that do not have the required background investigation (the FSO will make the determination by searching for a valid account for that person in DISS). If a valid account does not exist in DISS, the contracting company must submit to the USTRANSCOM Personnel Security Manager (through the CO or COR), an OF Form 306 (Declaration for Federal Employment), and a SF 85 (questionnaire for Non-Sensitive Positions) it's only sent after the FSO or equivalent reviews it for accuracy.

b) At the same time, the contractor company will coordinate and obtain electronic fingerprinting for their employee. The third-party Company will "electronically" capture the applicant's fingerprints, using the USTRANSCOM (SON, SOI, and ALC). Hardcopy fingerprint cards are not acceptable.

These steps shall be completed before the COR/Trusted Agent (TA) accesses the DOD Trusted Associate Sponsorship System (TASS), to create a CAC application.

Basic U. S. Citizen Contractor CAC Requirements:

1) Requires access on a continual basis of 6 months or more.
2) Contract personnel require access to a DoD facility or networks, either on-site or from a remote location.
3) Users need access to systems for platforms that requires CAC login or user authentication.

Basic Non- U. S. Citizens Contractor CAC Requirements:

1) Possess legal U. S. residency for a period of 3 or more years with a completed Tier 1 background investigation and fingerprint card. Also meet (as a direct/indirect DoD hire personnel) the investigative requirements for DoD employment as recognized through international agreements pursuant to subchapter 2131 of DoD 1400.25 (reference M).
2) Possess (as foreign military, employee or contract support personnel), a visit status and security assurance that has been confirmed, documented and processed I/A/W international agreements pursuant to DoDI 1400.25: Civilian Personnel Management.

CAC Applications:

1) The CAC applications must have an adjudicated Tier 1, Tier 3 or Tier 5 background investigation posted in DISS, or
2) An interim CAC may be approved when the contractor employee has a favorable fingerprint, name and criminal records check completed and has either a Tier 1, Tier 3 or Tier 5 background check "open" with OPM.

The TASS TA will not approve the CAC application in TASS until that TA has verified with the PSC, one of the above requirements.

11..8. Access to Scott Air Force Base or AMC Facilities

Upon receipt of the CAC, permanently assigned contractor personnel located at AMC at Scott AFB (SAFB), IL, may obtain the AF 1199 (Restricted Area Badge) if the employee meets the requirements set forth in SAFB Instruction 31-101. This stipulates that personnel who request AF 1199's be assigned physically on SAFB at least four (4) days a week with a desk

computer and phone before an AF 1199 will be issued. The Government will provide unrestricted access to facilities, consistent with security clearance and need to know, necessary for the on-site personnel to perform their work IAW the task order. Contractor personnel assigned on-site at USTRANSCOM will wear and display the Restricted Area badge at all times while in Government facilities. Visits to SAFB by contractor personnel who do not possess the CAC will be facilitated by the COR/CO sponsoring the employee through the online base access system.

11..9. Visits by Non-Assigned Contractors to AMC Buildings

Any visit(s) by contractor personnel not permanently assigned to this task order (i.e., company presidents, company security managers, contractor personnel not permanently assigned at SAFB, etc.) require an electronic visit request be submitted using DISS. DISS visits can be forwarded to the Security Management Office (SMO) code: AMC. The visit request shall annotate the contract title in the POC block of the visit request and the name/phone number of either the functional, PMO, COR or CO in the phone number block.

11..10. Visits by Permanently Assigned Contractors

Permanently assigned contractor employees on SAFB will require a visit request for the current period of performance posted in DISS to SMO provided by AMC PMO. The visit request will annotate the contract title in the POC block of the visit request and the name/phone number of either the functional, PMO, COR or CO in the phone number block. Upon in-processing permanently assigned contractors will require a copy of the DD Form 254 for this task order to show the classified access level for this task order and to assist in assigning permissions on restricted area badges.

11..10.1. Supplemental Notes Regarding Visit Information in DISS

Personnel requiring access to Government facilities will properly complete the "Visit Information" block in DISS. Otherwise, contractor employees will be denied access to the facility and classified and/or sensitive information. Also, prime contractors will annotate their contract number and subcontractors will provide the name of their Company, with the prime contract number they are assigned to by the Prime, in the "additional information" block of the Visit table. A valid "Reason for the Visit" must be stated and the "visit access" must not exceed that of the contract.

11..11. Security and Emergency Operations Training

Contractor personnel physically assigned at shall attend/complete the following training as prescribed by DOD, USTRANSCOM and Air Force Instructions: Employee Initial Security Briefing, Annual Security Awareness, OPSEC, DOD Antiterrorism Level I, Active Shooter, Emergency Operations and any other training required to perform work on Scott AFB. Contractor personnel assigned elsewhere shall attend security training established by their respective Government security offices and/or installations.

11..12. Additional Security Conditions

Contractors may be required to complete in-processing actions, pursuant to their workplace or duties, i.e., Restricted Area Badge (AF-1199) for building entry, Common Access Card, etc.

11..13. Derogatory Information.

If the Government notifies the contractor that the employment or the continued employment of any contractor personnel is prejudicial to the interests or endangers the security of the United States of America, that employee shall be removed and barred from the worksite. This includes security deviations/incidents and credible derogatory information on contractor personnel during the course of the task order's period of performance as noted in DISS. Personnel who have incident reports posted in DISS will be denied the ability to support the task order until the issues have been resolved and the incident has been removed in DISS. The contractor shall make any changes necessary in the appointment(s), at no additional cost to the Government. If any incident involves or may involve the mishandling of classified information or a potential Negligent Discharge of Classified Information, the USTRANSCOM Protection and Response Division (618-220-6538/6531) will be notified within 24 hours during the normal work week and within 72 hours if the incident occurs over the weekend.

11..14. Security Debriefing.

Contractor personnel physically working at SAFB, IL, or contractor employees possessing Government provided credentials, shall complete the out-processing checklist on the last day of the task order or upon termination or reassignment from duties under the current contract or task order. The following closeout tasks will be completed, before the contractor employee departs:

- Review of the contractor employee's personnel folder.
- Review and debrief the contractor employee's SF-312.
- Update and annotate DISS records reflecting the current status of the contractor employee at AMC.
- Surrender CAC cards (with a copy of the revocation notice from the COR or TA).
- Surrender the facility Restricted Area Badge (AF-1199) to the Protection Service Center.
- Contractor personnel shall have surrendered all Government supplies, materials and equipment to the COR.

11..15. NOTE TO THE PRIME CONTRACTOR FACILITY SECURITY OFFICER (FSO):

The prime contractor will forward the name, address, email address and telephone number of the Company FSO and backup to the USTRANSCOM Protection Programs Division TCJ3-MP to:

USTRANSCOM Protection Programs Division (Industrial Security) Points of Contact:

USTRANSCOM
Attn: TCJ3-MP 508 Scott Drive
Scott AFB IL 62225
Commercial: 618-220-6531/220-7892 (respectively)

USTCJ3-PR Approval:USTRANSCOM (Protections Programs Branch)

USTCJ3- PR Tracking #: USTRANSCOM-MP-0044-20

- **USTRANSCOM – Cyberspace Workforce Management**

11..1. In concert with DFARS 252.239-7001, Information Assurance Contractor Training and Certification, DoD 8570.01-M, Information Assurance Workforce Improvement Program, and

USTCI 6600.01, Policy for Cyberspace Workforce (CW) Management, the Contractor shall ensure all personnel performing cyberspace workforce role functions in support of or on DoD information systems, software, networks, and enclaves satisfy and maintain the appropriate DoD- approved baseline security certification and all applicable computing environment certification requirements commensurate with their current job duties in support of all environments (e.g., development, staging, client test, quality assurance, user acceptance testing, sandboxes, preproduction environments, and associated information system failover, contingency components, and infrastructure as code) in which they are performing work, to include off-site locations, throughout the contract performance period:

11..1.1. At least one DoD 8570.01-M mandated Information Assurance (IA) certification per defined role in Appendix E in the following categories: IA Technical (IAT), IA Management (IAM), and/or IA System Architect and Engineer (IASAE). Additional certification requirements exist for personnel supporting Cyber Security Service Provider (CSSP) functions (Analyst, Support, Responder, Auditor, Service Provider/Manager). A current list can be found at https://public.cyber.mil/cw/cwmp/dod-approved-8570-baseline-certifications/.

11..1.2. Contractor personnel shall hold at least one Computing Environment (CE) certification or certificate for the operating system(s) and/or security related tools/devices they support as defined by the contractor's cyberspace function listed in Appendix "X" satisfying one of the following categories:

1) Software development (e.g., java, .net. C++, python, Visual Basic, etc.)
2) Network support/defense (e.g., Splunk, Cisco, McAfee, etc.)
3) Cloud or virtualization (e.g., Azure, AWS, oracle, IBM, etc.)
4) Operating System (e.g., Microsoft, Linux, Solaris, etc.)
5) Application (e.g., database, backup, automation, webserver, network, proxy, firewall, etc.)

11..1.3. Contractor personnel shall participate in local training on USTRANSCOM procedures and operations practices upon arrival and a reoccurring annual basis. Contractor personnel who require certifications as outlined above must complete an on-the-job evaluation and provide proof of evaluation to the Contracting Officer Representative (COR) will validate the necessity for contractor personnel to attend USTRANSCOM-specific training and provide written certification to the USTRANSCOM Manpower and Personnel Directorate (TCJ1) that such training is USTRANSCOM-specific and required in order for contractor personnel to perform the requirements of their contract. Contractor personnel must also provide proof to the COR or designee of appropriate CE certification(s) and/or certificate(s) they support. The contractor shall provide, in the monthly Personnel Status report, information detailing the contractor personnel assigned, required certifications, and associated certification status.

11..1.4. Contractor personnel requiring privileged access (i.e., any elevated privilege beyond normal user-level access) must complete a Privileged Access Agreement, referred to herein as a Statement of Acceptance and Responsibilities (SOAR). A new SOAR must be executed prior to a role change that requires privileged access.

Contractor personnel will need to maintain certification status by completing continuous learning requirements as defined by the respective certification provider (e.g., ISC2, ISACA, CompTIA, etc). Contractor personnel will monitor current certification provider activity to see if they have imposed additional continuously learning requirements.

11..2. Contractor personnel who do not have current certification(s) or certificate(s) as specified in Appendix E for their specified roles shall be denied access to information systems unless a waiver has been granted by the USTRANSCOM Authorizing Official (AO).

11..2.1. DoD-approved baseline security certifications as delineated in DoD 8570.01-M are not eligible for an AO waiver.

11..2.2. The USTRANSCOM AO/PMOmay allow up to six months for contractor personnel to obtain DoD-approved certification(s) or certificate(s) for designated role requirements in situations of severe operational or personnel constraints. AO waivers must include an expiration date not to exceed six months and be documented in the individual's IA training record. Consecutive waivers for personnel are prohibited.

Appendix A: References
Defense Electronic Libraries:

- Acquisition Notes: http://acqnotes.com
- Assist – Quick Search: http://quicksearch.dla.mil
- Official Website of the Joint Chiefs of Staff (JCS): https://www.jcs.mil/
- Department of Defense: http://www.esd.whs.mil/dd/dod-issuances/
- Federal Registry: https://www.federalregister.gov/
- Joint Electronic Library: https://www.jcs.mil/Doctrine/
- Federal Information Processing Standards (FIPS) and National Institute of Standards and Technology (NIST): https://csrc.nist.gov/publications
- Military Standards (MIL-STD): https://www.dau.mil/
- Committee on National Security Systems (CNSS): https://www.cnss.gov/CNSS/issuances/Instructions.cm
- Institute of Electrical and Electronics Engineers (IEEE) Publications: https://www.ieee.org/publications_standards/index.html

Governing Guidance and Directives:

- American National Standards Institute (ANSI)/Electronic Industries Alliance (EIA) 748: Earned Value Management, current edition
- CJCS Instruction 5123.01H, CHARTER OF THE JOINT REQUIREMENTS OVERSIGHT COUNCIL (JROC) AND IMPLEMENTATION OF THE JOINT CAPABILITIES INTEGRATION AND DEVELOPMENT SYSTEM (JCIDS), August 31, 2018
- CJCS Instruction 6510.01F, Information Assurance (IA) and Support to Computer Network Defense (CND), June 9, 2015
- CJCSM 3213.02D, Joint Staff Alternative Compensatory Control Measures (ACCM) Program Management Manual (Limited Distribution)
- CJCSM 6510.01B, Cyber Incident Handling Program, 10 July 2012
- Data Item Management-81861, Data Item Description: Integrated Program Management Report (IPMR), June 20, 2012
- DD Form 254, Contract Security Classification Specification, November 1, 2017
- Defense Federal Acquisition Regulation Supplement, current edition
- DOD 5200.08, Security of DoD Installations and Resources and the DoD Physical Security Review Board (PSRB), Change 3, November 20, 2015
- DoDM 6025.18, Implementation of The Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule in DoD Health Care Programs, March 13, 2019
- DoD Instruction 8500.01, Cybersecurity, Change 1, October 7, 2019
- DoD Instruction, 8510.01, Risk Management Framework (RMF) for DoD Information Technology (IT), Change 2, July 28, 2017

- DoD Directive 5230.25, Withholding of Unclassified Technical Data from Public Disclosure, December 28, 2016
- DoD Instruction 8320.02, Data Sharing, in a Net Centric Department of Defense, August 5, 2013
- DoD Instruction 1100.22, Policy and Procedures for Determining Workforce Mix, Change 1, December 1, 2017
- DoD Instruction 2000.12, DoD Antiterrorism (AT) Program, Change 3, May 8, 2017
- DoD Instruction O-2000.16, DoD Antiterrorism (AT) Program Implementation: DoD AT Standards, Volume 1, Change 2, November 20, 2019
- DoD Instruction O-2000.16, DoD Antiterrorism (AT) Program Implementation: DoD Force Protection Condition (FPCON) System Volume 2, May 8, 2017
- DOD Instruction 5025.13, DOD Plain Language Program, January 23, 2020
- DOD Instruction 8330.01, "Interoperability of Information Technology (IT), Including National Security Systems (NSS)," December 18, 2017
- DOD Instruction 8500.01, "Cybersecurity," March 14, 2014
- DOD Instruction 8510.01, "Risk Management Framework (RMF) for DOD Information Technology (IT)," July 28, 2017
- DOD Instruction 8520.02, "Public Key Infrastructure (PKI) and Public Key (PK) Enabling," May 24, 2011
- DOD Instruction 8551.01, "Ports, Protocols, and Services Management (PPSM)", July 27, 2017
- DOD Instruction 8582.01, "Security of Unclassified DOD Information on Non-DOD Information Systems," October 27, 2017
- DOD Manual 1000.13, Volume 1, "DOD Identification (ID) Cards: ID Card Life- Cycle," January 23, 2014
- DoDM 5200.01, Volume 1_DAFMAN 16-1404, Volume 1, Information Security - Overview, Classification, and Declassification
- DoDM 5200.01, Volume 2_DAFMAN 16-1404, Volume 2, Marking of Classified Information
- DoDM 5200.01, Volume 3_DAFMAN 16-1404, Volume 3, Protection of Classified Information
- DoDI 5200.48_DAFI 16-1403, Controlled Unclassified Information (CUI)
- DOD 5200.08-R, Change-1, DoD Physical Security Program, May 27, 2009
- DFARS 252.205-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting
- DFARS 239.73, Requirements for Information Related to Supply Chain Risk, February 15, 2019

- DoDM 5200.02_AFMAN 16-1405
- DoDM 5220.22, Volume 2_DAFMAN 16-1406, Volume 2, "National Industrial Security Program: Procedures for Government Activities Relating to Foreign Ownership, Control, or Influence (FOCI)," April 17, 2014
- DOD Standard MIL-STD-881C, "Work Breakdown Structures (WBS) for Defense Materiel Items," October 3, 2011
- FD Form 258, Fingerprint Card
- Office of Management and Budget Circular A-11, "Preparing, Submitting, and Executing the Budget," current edition
- USTRANSCOM Instruction 31-02, "Security Classification Guide," October 9, 2015
- USTRANSCOM Instruction 31-11, "Security Program," September 21, 2010
- USTRANSCOM Instruction 31-12, "Operations Security," February 19, 2015
- USTRANSCOM Instruction 33-1, "Information Systems Security Education, Training, and Awareness Program," March 27, 2017
- USTRANSCOM Instruction 33-48, "Data Management Policy and Responsibilities," February 16, 2016
- USTRANSCOM Instruction 33-58, "Cyber Workforce Management," February 26, 2016
- Scott Air Force Base: AF Instruction 31-101_AMC, January 4, 2014
- FIPS 199, "Standards for Security Categorization of Federal Information and Information Systems," February 2004
- FIPS 200, "Minimum Security Requirements for Federal Information and Information Systems," March 2006
- NIST SP 500-267B Revision 1, "USGv6 Profile," November 2020
- NIST SP 800-18 Revision 1, "Guide for Developing Security Plans for Federal Information Systems" February 2006
- NIST SP 800-30 Revision 1, "Guide for Conducting Risk Assessments," September 2012
- NIST SP 800-37 Revision 1, "Guide for Applying the Risk Management Framework to Federal Information Systems: a Security life Cycle Approach," June 5, 2014
- NIST SP 800-53, Revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations," January 22, 2015
- NIST SP 800-53A Revision 4, "Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans," December 18, 2014
- NIST SP 800-60 Volume 1, Revision 1, "Guide for Mapping Types of Information and Information Systems to Security Categories," August 2008
- NIST SP 800-61 Revision 2, "Computer Security Incident Handling Guide," August 2012
- CNSS Instruction 1253, "Security Categorization and Control Selection for National Security Systems," March 27, 2014

- 12207.0-1996 IEEE/EIA Standard Industry Implementation of International Standard ISO/IEC 12207: 1995 (ISO/IEC 12207) Standard for Information Technology Software Life Cycle Processes. Superseded by: 12207-2008 – Standard for Information Technology – Software Life Cycle Processes
- 12207.1-1997 - Industry implementation of International Standard ISO/IEC 12207: 1995. (ISO/IEC 12207) Standard FOR Information Technology - Software Life Cycle Processes
- - Life Cycle Data superseded by: 15289-2017: 15289-2017 - ISO/IEC/IEEE Draft International Standard - Systems and software engineering -- Content of life-cycle information items (documentation)
- Executive Order (E.O.) 13691 of February 13, 2015. Promoting Private Sector Cybersecurity Information Sharing
- DODD 8140.01, Cyberspace Workforce Management https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/814001p.pdf?ver=2019
- -06-06-120639-863
- DOD 8570.01-M, Information Assurance Workforce Improvement Program https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/857001m.pdf
- USTCI 6600.01, Policy for Cyberspace Workforce (CW) Management (under review). https://static.e-publishing.af.mil/production/1/saf_cn/publication/afman17-1303/afi17-1303.pdf
- DFARS Subpart 239.71, Security and Privacy for Computer Systems https://www.acq.osd.mil/dpap/dars/dfars/pdf/r20080110/239_71.pdf

Appendix B: List of Government Furnished Information

The information listed below is available in the Technical Data Package. Upon contract award, the Government will provide the Contractor with information not furnished in the RFP pertinent to completing this contract.

- Attachment 1_Reserved; Left Blank at this Time
- Attachment 2_Reserved; Left Blank at this Time

Appendix C: Acronyms

Acronym	Definition
AAR	After Action Report
ACAS	Air Carrier Analysis Support
AFFARS	Air Force Federal Acquisition Regulation Supplement
AI	Artificial Intelligence
ALM	Application Lifecycle Management
AMC	Air Mobility Command
AMT	Agile Management Tool
AP	Assessment Procedure
ASI	Authorized Service Interruption
ATO	Authority to Operate
CAC	Common Access Card
CARB	Commercial Airlift Review Board
CCI	Control Correlation Identifier
CI/CD	Continuous Integration/Continuous Delivery
CIL	Critical Information List
CJCS	Chairman Joint Chiefs of Staff
CJCSI	CJCS Instruction
CJCSM	CJCS Manual
CM	Configuration Management
CMMI	Capability Maturity Model Integrated
CMP	Configuration Management Plan
CO	Contracting Officer
COA	Course of Action
COOP	Continuity of Operations Plans
COR	Contracting Officer's Representative
COTS	Commercial Off The Shelf
CR	Change Requests
CRAF	Civil Reserve Air Fleet
CCE	Cloud Computing Environment
CSP	Cloud Service Provider
CST	Client Support Technician
CUI	Controlled Unclassified Information
CVE	Common Vulnerabilities and Exposures
DAST	Dynamic Application Security Test
DBA	Database Administration
DCAR	DoD Centralized Artifact Repository
DEERS	Defense Enrollment Eligibility Reporting
DFARS	Defense Federal Acquisition Regulation Supplement

DDS	Defense Distribution System

DISA	Defense Information Systems Agency
DNS	Domain Name Service
DOD	Department of Defense
DODAF	Department of Defense Architecture Framework
DoDD	DoD Directive
DoDI	DoD Instruction
DoD-M	DoD Manual
DTMO	Defense Transportation Management Organization
EIT	Electronic and Information Technology
EAS	Environment Administration Support
ESR	Employee Status Report
EULA	End-user License Agreement
FAA	Federal Aviation Administration
FAR	Federal Acquisition Regulation
FCL	Facility Clearance
FMO	Functional Management Office
FOUO	For Official Use Only
FSA	Functional System Administrator
FY	Fiscal Year
GAT	Government Acceptance Testing
GFE	Government Furnished Equipment
GFI	Government Furnished Information
GFP	Government Furnished Property
GFS	Government Furnished Software
GIG	Global Information Grid
GPS	Government Purpose Software
GFM	Government Functional Manager
GSM	Government Systems Manager
HBSS	Host Based Security System
IA	Information Assurance
IAM	Information Assurance Management
IATT	Interim Authority To Test
IAVA	Information Assurance Vulnerability Alert
IAVM	Information Assurance Vulnerability Management

Appendix D: Non-Disclosure Agreement

NONDISCLOSURE AGREEMENT AND AGREEMENT TO DISCLOSE POTENTIAL CONFLICTS OF INTEREST FOR CONTRACTOR EMPLOYEES ON USTRANSCOM CONTRACTS

NOTE: This Agreement is a standard agreement designed for use by contractor (including sub-contractor) employees assigned to work on USTRANSCOM/AMC contracts. Its use is designed to protect non-public Government information from disclosure, identify potential conflicts of interest, and prevent violations of federal statutes/regulations. The restrictions contained in this agreement also serve contractors by promoting compliant behavior that keeps contractors eligible to compete for Government contracts. In addition to the potential impact on future business opportunities, failure to abide by this agreement could result in administrative, civil, or criminal penalties specified by statute or regulation.

1. I, , currently an employee of , hereby agree to the terms and conditions set forth below.

2. I understand that I may have access to confidential business information, contractor bid or proposal information (as defined by FAR 3.104-1), and/or source selection information (as defined by FAR 2.101) either for contract performance, as a result of working in a USTRANSCOM/Gov't facility, or of working near USTRANSCOM/AMC personnel, contractors, visitors, etc. I fully understand that such information is sensitive and must be protected in accordance with 41 U.S.C.§2101-§2107 and FAR 3.1.

3. In the course of performing under contract/order # or some other contract or sub-contract for USTRANSCOM, I agree to:

    a) Use only for Government purpose any and all confidential business information, contractor bid or proposal information, and/or source selection sensitive information to which I am given access. I agree not to disclose "non-public information" by any means (in whole or in part, alone or in combination with other information, directly, indirectly, or derivatively) to any person except to a US Government official with a need to know or to a non-Government person (including, but not limited to, a person in my company, affiliated companies, sub-contractors, etc.) who has a need to know related to the immediate contract/order, has executed a valid form of this non-disclosure agreement, and receives prior clearance by the Contracting Officer. All distribution of the documents will be controlled with the concurrence of the Contracting Officer. I understand that misuse of non-public information is subject to penalties established in applicable laws, regulations, or Government-wide policies.

b) “Non-public information,” as used herein includes confidential or proprietary business information ((; advance procurement information (future requirements, acquisition strategies, statements of work, budget/program/planning data, etc.); source selection information (proposal rankings, source selection plans, contractor bid or proposal information); information protected by the Privacy Act (social security numbers, home addresses, etc.); sensitive information protected from release under the Freedom of Information Act (pre-decisional deliberations, litigation materials, privileged material, etc.); Export Controlled Items (as defined by DFARS 252.225-7048); Controlled Unclassified Information (as defined by 32 CFR 2002); Covered Defense Information (as defined by DFARS 204.7301); and information otherwise protected from disclosure by statute, Executive order or regulation designated as confidential that has not been released to the general public and has not been authorized for such release.

c) Nonpublic information also includes trade secrets as defined by 18 U.S.C. §1839. The term "trade secret" means all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if –

(1) the owner thereof has taken reasonable measures to keep such information secret; and

(2) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, another person who can obtain economic value from the disclosure or use of the information;

d) Not use such information for any non-Governmental purposes, including, but not limited to, the preparation of bids or proposals, or the development or execution of other business or commercial ventures.

e) Store the information in such a manner as to prevent inadvertent disclosure or releases to individuals who have not been authorized access to it.

4. I understand that I must never make an unauthorized disclosure or use of confidential business information, contractor bid or proposal information, and/or source selection sensitive information unless:

(a) The information has otherwise been made available without restriction to the Government, to a competing contractor or to the public.

(b) The Contracting Officer determines that such information is not subject to protection from release.

5. I agree that I shall not seek access to "non-public information" beyond what is required for the performance of the services I am contracted to perform. I agree that when I seek access to such information, attend meetings, or communicate with other parties about such information, I will identify myself as a contractor. Should I become aware of any improper or unintentional release or disclosure of "non-public information", I will immediately report it to the Contracting Officer in writing. I agree that I will return all forms (including copies or reproduction of original documents) of any "non-public information" provided to me by the Government for use in performing my duties to the control of the Government when my duties no longer require this information.

6. Because the Government expects unbiased judgment and recommendations from contractors performing work under its contracts and orders, I agree to advise the Contracting Officer of any actual or potential personal conflicts of interest I may have related to any work I perform under this contract/order with the government. Personal conflicts of interest include any matter in which I or my spouse, minor child, or household member has a financial interest. A financial interest is any interest in, or affiliation with, a prime contractor, subcontractor to a prime contractor, any offerors, or any prospective subcontractor to any offeror for the program, contract, or other matter for which I am performing a support task under this contract. The financial interest can take the form of any ownership interest (including but not limited to: stock; ownership of bonds; vested or unvested retirement benefits; a loan or other financial arrangement that is other than an arm's-length transaction; employment, or an arrangement concerning prospective employment including negotiations therefore; or any non-arm's length loan, any gift from or other non-arm's length financial arrangement with any person who is directly communicating with the government on behalf of the prime contractor, subcontractor, or any prospective subcontractor or offeror). With respect to conflict-of-interest disclosures required under this agreement, a financial interest in, or affiliation with, the prime contractor that is my employer under this contract does not have to be disclosed to the Contracting Officer. If any potential conflicts of interest, real or otherwise, do present themselves, then I shall immediately disclose the pertinent information to the Contracting Officer. I acknowledge that my access to certain non-public information may disqualify me or my company from certain future contracts with the U.S. Government.

7. I understand that this agreement is personal to me and shall survive and remain in full force and effect notwithstanding any change in current employment.

By signing below, I certify that I have read and understand the terms of this Non-Disclosure Agreement and Agreement to Disclose Potential Conflicts of Interest, and voluntarily agree to be bound by its terms.

Signature of Contractor Employee **Date**

Printed Contractor Employee Name

Government Contracting Officer's Representative **Date**

Appendix E: Contractor Cyberspace Workforce Management Training and Certification

Task Area	Cyberspace Function	C.L. S/TS	IAT I	IAT II	IAT III	IAM I	IAM II	IAM III	IASAE I	IASAE II	IASAE III	CSSP A	CSSP IS	CSSP IR	CSSP AU	CSSP SPM	Computing Environment Cert
1	Task Order Management																X
2	Configuration Management and Quality Assurance																X
3	Software Development Support			X	X*												X
4	Monitoring and Production Application Support			X	X*												X
5	Risk Management Framework (RMF) Support			X	X*		X										X
6	Build Development Environment			X	X*					X							X
	Contract Phase-In/Transition			X	X*												X

- *All team members must meet minimum requirement of IAT II, but team technical lead role and DevSecOps ~~L~~ead roles requires IAT III.

Appendix F: Technology Landscape

The Contractor teams shall be proficient in using and managing the following languages and tools. As technology evolves, so must the technical expertise and the tools used by the team. It's expected the teams will evolve as technology evolves throughout the period of performance of the Contract. The table below provides the primary tools (not all inclusive) that are provided by the Government and are used to support the portfolio of applications. The description of each application further identifies the tools used to allow the Contractor to identify the skillsets required to support the portfolio. The Contractor shall not use any components, subcomponents, software, tools, or containers unless listed in the table below or approved by the COR in writing.

Name	Manufacturer	Function
Angular	Google - Open Source	A structural framework for dynamic web apps
Agile Methodology	Open Source	Agile development practices
Apache HTTP Server	Apache - Open Source	Web Server
Apache Tomcat Server	Apache - Open Source	Application Server
Arcserve	Arcserve	Server/VM backup software; Data Protection
Artifactory	Jfrog	Universal Repository for Artifacts
Chef	Chef	configuration management tool
Cloud Service Providers (CSP)	Various	Cloud platforms, also as prescribed by the Government
CompoDoc	Open Source	Angular Documentation tool
Docker	Open Source	Operating System level virtualization tool - "containers"
ERWin	ERWin	Data modeling tool
Fortify Software Center (SSC)	Micro Focus	Security static code analysis testing tool
Fortify Static Code Analyzer (SCA)	Micro Focus	Security static code analysis testing tool
GitLab	GitLab Inc	Web based Devops Tool and Git Repository
HTML		Web programming language
Java		Programming Language
Jenkins	Open Source	Automation Server -

		build/test/deploy
Jira	Atlassian	Project management tool
JSP		Programming language
JUnit	Open Source	Java unit testing framework
Kubernetes		Container build/deploy/scale/manage tool
Maven	Apache - Open Source	Project Object management tool - software build
Mockito	Open Source	Java testing framework
OpenJDK	Open Source	Open source Java Class Library/compiler (javac).
Oracle Data Guard	Oracle	Database Replication
Oracle Enterprise Database	Oracle	Database
PL/SQL	Oracle	Database Programming Language
Red Hat Linux	Red Hat	Operating System
Risk Management Framework (RMF)	Government	As required to support
Selenium	Open Source	Web Testing Framework
SoapUI	ReadyAPI	Web service Testing tool
SonarQube	SonarSource	tool for continuously inspecting the Code Quality
Spring Framework	Open Source	Java Framework
Toad for Oracle	Quest	Oracle development tool
VMWare vCenter	VMware	Server Management Software
VMWare vSphere	VMware	virtualization server platform

Appendix G: PWS Incorporated Exceedances

Attention Schedule Contractors:

Aspects of the schedule contractor's quote that are incorporated into the resultant award will be placed in this document.

The Government, if it is in its best interest, reserves the right to use this attachment to incorporate all beneficial aspects of the awardee's quote (to include all above minimum attributes, performance levels, or capabilities) for which evaluation credit was given into the PWS. The Government may use (but is not limited to) the following methods of incorporation:

The following is an example of how the Government may incorporate aspects of the awardee's quote as a narrative into the PWS in order to ensure that they are delivered during performance:

"The contractor shall perform the XX process as described in their quote (provide quote reference)."

The following is an example of how the Government may incorporate aspects of the awardee's quote by addendum to the PWS paragraphs in order to ensure that they are delivered during performance:

PWS Para 5 Addendum

If the addendum applies to Task X, and Task X is comprised of paragraph 5 and its subparagraphs 5.1 through 5.9, the addendum paragraph would be 5.10 and following.

The following is an example of how the Government may incorporate aspects of the awardee's quote/ into the PWS Services Summary in order to ensure that they are delivered during performance:

PWS Services Summary Addendum

Performance Objective	Quote Reference	Performance Threshold
State performance or capability exceedances above mandatory threshold (minimum) from offeror's quote.	State quote/proposal reference.	State threshold quoted by offeror or agreed upon during discussions/interchanges.

The Government may copy and paste verbatim from the awardee's quote/proposal.