FA3002-18-C-XXXX

Air Education and Training Command Technology Integration Division (A5T) Legacy Information Systems Support

6 Mar 2018

NETCENTS-2 SOLUTIONS

Application Services – Full & Open / Small Business Companion
Air Education and Training Command
Technology Integration Division (A5T)
Legacy Information Systems (IS) Support
Task Order Performance Work Statement (PWS)

Name:	Vashti Hawkins
Organization:	AETC/A5T
Address:	61 Main Circle, Suite 2 JBSA – Randolph, TX 78150

Executive Summary

HQ Air Education and Training Command (HQ AETC) recruits, assesses, commissions, trains, and educates Air Force (AF) enlisted and officer personnel. AETC provides basic military training, initial and advanced technical training, flying training, professional military and degree-granting professional education. AETC conducts joint, medical service, readiness and AF security assistance training. AETC/A5T manages a number of information systems used to support AETC's core mission to provide Recruiting, Training, and Education capabilities to the Air Force.

NETCENTS-2 Application Services Task Order PWS

Air Education and Training Command Technology Integration Division (A5T) Legacy Information Systems Support

1. PURPOSE

HQ AETC Technology Integration Division (A5T) requires database administrator; network administrator, software analysis and sustainment; product testing, product review, and process audit services; beta test; production support and cybersecurity oversight to maintain government-owned training information systems that support HQ AETC mission.

2. SCOPE

The objective of this effort is to acquire information technology sustainment support services for AETC/A5T Legacy Information Systems.

For purposes of this PWS, sustainment is defined as maintaining the existing software and hardware infrastructure to include maintaining existing software capabilities upgrades (e.g., versions, updates, service packs), and facilitating replacement or repair of government furnished equipment (GFE) (e.g., servers, backup systems) to meet operational suitability requirements and mandates. These legacy system baselines are frozen except for items required for hardware and software security. Any new capabilities must be proposed in writing to the A5T Division Chief and approved prior to commencement of work. Sustainment includes the integration of all sustained software and hardware changes/updates. During the performance period the hardware, software, communication, facilities and ancillary equipment environment may change or be modified (e.g., server locations may be moved, new communications circuits may be added/changed); normal and reasonable sustainment tasks to adjust for these changes are within scope.

Software sustainment encompasses all aspects of supporting, maintaining, and operating the software aspect of a system. It is a superset of software maintenance activities, which includes corrective, adaptive, preventive, and perfective modifications. Software sustainment also addresses other issues not typically included in maintenance such as operations, documentation, deployment, security (e.g., scans, patching known vulnerabilities, etc.), configuration management, user and operator/administrator training, and user support.

The contractor shall also provide service support and enhancements to several government-owned information systems.

2.1. Advanced Distributed Learning Services (ADLS)

ADLS is a Learning Management System (LMS) an Air Force Enterprise solution that delivers online courses, tracks learner progress, and provides reports for individuals, supervisors, training managers, and commanders of the AF, the DoD, and Joint organizations (790,000 users). ADLS currently consists of 18 partner sites which deliver: MAJCOM Courses; Technical & Flying Training; AF Ancillary Training; Expeditionary Skills Training; Language and Culture Training; Career Development Courses; Professional Military Education; Functional Area Courses. HAF/A1 has directed the ADLS to be the Air Force Universal Ancillary Training delivery and tracking system. The ADLS also provides the platform for the Air Force Training Record, an electronic training record for On-the-Job Training for the Mission Support Functional Communities. This effort shall require leveraging existing functionality of the government provided course delivery engine software and integrating government-owned information systems to support AETC. ADLS is hosted at the Defense Information Systems Agency (DISA) which provides network access and manages the administration of those network devices.

2.2. Promotion and Testing System (PTS)/Occupational Analysis (OA)

PTS is a multi-featured relational database system, with associated application software suite (to include an array of statistical, scoring, management and report functions), that facilitates senior Air Force (AF) leadership decision making by accomplishing the following empirical statistical data functions:

- Analyze personnel data to define AF job classifications and associated training programs.
- Optimize enlisted promotion test construction.
- Produce and deliver the enlisted promotion testing material.
- Validate AF enlisted promotion testing results.

- Collect and compile occupational tasks and testing importance analysis.
- Quantify, organize, and analyze report data collected from job task inventories and occupational surveys.
- Report test planning data, as well as, select statistical reports on population for targeting occupational surveys.
- Create surveys and produces high quality digital products for transfer to other Air Force approved systems or electronic storage.
- Track survey status and return rates of surveys.

PTS functions utilize customizable Commercial Off-The-Shelf (COTS) software that has been certified for placement on the Air Force Evaluated/Approved Product List (AF EPL).

2.3. Service Now

HQ AETC requires support for the local and Defense Information Systems Agency (DISA) hosted instance of ServiceNow. The ServiceNow application automates help desk functions and Information Technology System Management (ITSM) processes supporting the AETC Recruit, Train, and Educate mission systems. A system administrator/functional system administrator and ServiceNow Configuration manager are required to sustain and support product testing, product review, and process audit services; and production support to maintain the government-owned instance of the ServiceNow application. The functional systems administrator functions in direct support of the unit’s operational mission, to include support of ServiceNow application operations and software configuration, database admin, systems security, and communications to maintain visibility of the system’s health and lifecycle indicators.

2.4. Cybersecurity Specialist

The required non-personal support services shall be provided as described in this PWS, and may evolve as the HQ AETC missions and operational objectives evolve in response to strategic Secretary of the Air Force, Office of Information Dominance and Chief Information Officer (SAF/CIO A6) guidance and direction. The contractor shall provide a Cybersecurity Professional to fulfill the role as the organizational cybersecurity manager with functional oversight responsibilities. As the cybersecurity manager, shall manage the cybersecurity program for all AETC Technology Integration division systems under the Information System Owner (Technology Integration Division Chief) and monitor the information systems ISSOs providing information assurance activities and support service.

3. REQUIREMENT(S)/DESCRIPTION OF SERVICE(S)

3.1 Systems Sustainment

Systems sustainment requirements must comply with applicable documents and standards specified in Section 8 of this TO PWS.

The contractor shall design, develop, test and package systems and software changes as well as provide problem resolutions for the existing system. The contractor shall maintain the current baseline of the system and provide software change and problem fixes to these baselines as approved prior to start of work. The contractor shall provide to the Government all developed, modified, or converted source modules, processes, programs, scripts, operating instructions, databases, system files, documentation, test files and test conditions used to develop each approved systems change request. Specific tasks may include the following:

- Maintain existing systems and environments IAW disciplined engineering practices and sustain applications, databases and interfaces in compliance with applicable AF/DoD standards.

- Support system sustainment activities to include maintaining existing legacy information systems and environments and to sustain applications, databases and interfaces.

- Provide application services to support, maintain and operate systems or services.

The contractor shall review system performance, reported issues, provide recommendations and implement fixes as prioritized by the contracting officer representative (COR).

The contractor shall provide to the contracting officer (CO) and the COR with sustainment plans to address each section below. Each plan shall be provided NLT 45 calendar days after contract award. The plans shall be revised annually thereafter (NLT 31 December of each calendar year), if changes are required. The planned deliveries for each product and/or document shall be IAW Deliverables described under Section 8.

3.0 SOFTWARE DEVELOPMENT LIFE CYCLE

The methodology that will be used by the legacy sustainment team to develop/modify new code modules will be the same standard five steps that are performed for sustainment releases -- each with a specific goal that will culminate with the timely completion of the development task and the required documentation.

3.1 Pre-Planning

The Pre-Planning phase of code modifications will take place as soon as the modification to the contract is awarded for the specific functional module. During the Pre-Planning phase, the team will use the requirements listed in the PWS and determine the software and infrastructure changes for the module. The COR will provide feedback and coordinate any necessary changes to meet program requirements, and approve/disapprove the plan. During the Pre-Planning phase the tasking proposal will be evaluated to insure that the scope of work necessary to complete the tasking does not exceed the allocated time required for completion of the Release Analysis, Design/Build Test, and Deployment cycle. Therefore the target timeframe for this coordination and compilation is 10 work days from submission of the Planned Maintenance Report.

Approved Software Development Plan

Project Plan/Schedule

3.2 Analysis

The Analysis phase will consist of a more in-depth evaluation of the requirements for the functional module. The I&ST will thoroughly examine each requirement, evaluate the scope and complexity and the required resources, and identify further information that may be required to complete this phase or the tasks in general. Any deficiencies will be identified and coordinated and necessary adjustments will be made at this time. The team will draft a change proposal before preforming any modifications to the system. They will update the requirements as they become more clearly recognized. The contractor will provide documentation regarding deployment; risks will be identified, analyzed, recorded, managed, and reviewed throughout the release cycle.

The end of this phase will be signified by the government approval of developed requirements, timelines, and acknowledgement of identified risks.

Analysis Phase Inputs

- Approved Software Development Plan
- Project Plan/Schedule
- PWS Requirements

Analysis Phase Outputs

- Approved Project Plan/Schedule
- Outstanding deficiencies and risk assessments
- Draft System Design/Architecture Document (defined in Software Sustainment Plan)

3.3 Design/Build

During the design and build phase of the development cycle, the contractor shall prepare written changes to the AETC A5T hardware and software architecture to satisfy the approved requirements developed in the Analysis phase. The contractor shall maintain applications, procedures, triggers, systems administration structures, interfaces, reports, and any required code necessary to institute the approved requirements.

During this phase, the team will coordinate and work closely with other teams to insure a smooth transition to the testing phase of the release cycle. Design and Build Phase Inputs

- PWS Requirements
- Approved Project Plan/Schedule
- Draft System design/architecture document
- Outstanding deficiencies and risk assessments

Design and Build Phase Outputs

- Coded changes to the APPLICATION baseline
- Development testing results
- Test plans and test procedures (2 weeks prior to test phase)
- Revised Project Plan and Schedule (as required)
- Approved Requirements Document

3.4 Test

The Test representative for the development effort will work closely with the Test Lead to ensure standard practices are being correctly followed and adequate testing is being accomplished, and with the Product Development Lead to ensure all identified problems are resolved. As new builds are provided throughout the development effort, the software will be installed on a testing instance at the integration center and tested to ensure that the new module meets requirements and functions without error. Release testing will also be accomplished to validate the build sequence. Any problems that cannot be resolved, are not directly associated to the build, or have been determined to be fixed at a later time, will be placed on the Known Defect list for submission with the completed module.

During this phase of the development cycle the user training modules are also finalized. The team will be involved in the development and testing processes and have developed the required user and training materials to accompany the software delivery. In addition, user release notes will be developed to insure comprehensive documentation of changes can be made available to the ADLS/PTS/OA and Service Now communities.

Upon completion of the test phase, the Test Lead will turn the tested content over to AETC A5T Service Validation and Testing for Acceptance Testing. This will include an environment that contains the version anticipated for release and all current documentation to include release notes. Test Phase Inputs

- Coded changes to application Baseline
- Development test results
- Approved Requirements Document
- Approved test plans and test procedures

Test Phase Output

- Tested and fixed application baseline
- Known defect list
- application baseline and inputs for IATO testing
- Completed test plans Quick look report

Test report

Updated Requirements Document

3.5 Deployment

The deployment phase is the phase in which final preparation is made for fielding the new module as planned. Throughout the Design/Build and Test Phases, the software development team will be in constant coordination with the COR to develop and finalize the release build. This constant communication is imperative to insure all software and hardware changes are applied in a consistent and non-destructive manner, all dependencies are identified and complete and accurate deployment instructions are generated. During the Deployment Phase, government operations section, i.e. Applications Management, will conduct an in-depth audit of release files to insure the latest versions of all changed modules are available and properly stored in the version management system. Once audited and identified, the proper authority will schedule a pre-release meeting a week prior to the scheduled release date. At this time, all key personnel will step through the final deployment instructions and review them for accuracy. The release files will be identified, deployment packages built, and final release times determined. Deployment Phase Inputs

- Tested and fixed Baseline
- Completed Test Plans
- Final Requirements Document Deployment Phase Outputs
- Fielded Baseline

- Version Description Documents
- Final Approved Requirements Document

3.1.1. Software Sustainment Plan

The contractor shall sustain all Legacy Information Systems software and create a Software Sustainment Plan to serve as the basis for activities under this work area. Contractor topics in the plan shall include but are not limited to:

- How the contractor shall conduct analysis to use COTS/GOTS software to accomplish engineering and integration activities
- How the contractor shall coordinate with and leverage HQ AETC A5T processes and functions to accomplish the tasks identified in this plan (e.g., coordination with Data & Architecture Function for development of architecture artifacts, coordination with Information Security process for development of security artifacts, etc.)
- How the contractor shall engineer (schedule, design and build) software changes to any of the legacy information systems architecture IAW standard software sustainment/development lifecycle practices to meet AETC functional and governance requirements. This shall include documentation/coordination of requirements, design, and testing (e.g., unit testing shall include peer review).
- How the contractor shall integrate the assigned National Institute of Standards and Technology (NIST) security controls, control correlation identifiers, and DoD/AF overlays.
- How the contractor shall provide system architecture and produce all required Operational Views (OVs), System Views (SVs), Data and Information Views (DIVs), Service Views (SvcVs), & Standard Views (StdVs) documents or other documentation IAW Department of Defense Architecture Framework (DoDAF) 2.02 (http://dodcio.defense.gov/Library/DoD-ArchitectureFramework/).
- How the contractor shall test COTS/GOTS integrated software. This shall include test plans, test procedures, and expected test results prepared and submitted for management approval prior to every software release. The test plan, test procedure, and test reports shall be published and coordinated IAW the Software Sustainment Plan.
- How the contractor shall deploy COTS/GOTS software IAW HQ AETC A5T Deployment Policy. This shall include site surveys, operational readiness planning, fielding plan, and component delivery and installation. A release Version Description Document (VDD) shall summarize the results of the delivery to the government. The plan shall include the software delivery method the contractor plans on using to push new software to the field.
- How the contractor shall acquire new integrated capabilities while sustaining existing software
- How the contractor shall maintain and upgrade existing suite of software applications and minimize cyber and end-of-life (EOL) security risks
- How the contractor shall plan, execute and report to the government on software sustainment activities
- How the sustainment work programs shall evolve near and long term
- Planning to minimize the software impacts on the business process and the overall enterprise architecture

- How the contractor shall publish and gain approval from A5T for software release schedules and contents, scheduled hardware maintenance that affects systems availability, and hardware installations
- How the contractor shall protect privacy information, including Personally Identifiable Information (PII). The work in this task order requires access to sensitive but unclassified systems and Personally Identifiable Information (PII). The Contractor must protect IAW the following regulations:

  ○ AFI 33-332 - *Air Force Privacy And Civil Liberties Program* ○

  DoD 5400.11-R - *DoD Privacy Program*

Products and documentation shall be published IAW the Software Sustainment Plan. **3.1.2.**

Hardware Sustainment Plan

The contractor shall sustain all legacy information systems hardware and associated components. Hardware sustainment includes all components necessary to sustain legacy information systems operations on the AFNet or other Network. The contractor shall create a Hardware Sustainment Plan to serve as the basis for near- and long-term activities under this work area. Contractor topics in the plan shall include but are not limited to:

- How the contractor shall update and/or change out components while sustaining the existing hardware configuration
- How the contractor shall plan, execute and report to the government on hardware sustainment activities
- How the contractor shall coordinate with and leverage HQ AETC A5T processes and functions to accomplish the tasks identified in this plan (e.g., coordination with Data & Architecture Function for development of architecture artifacts, coordination with Information Security process for development of security artifacts, etc.)
- How the hardware sustainment work programs shall evolve near and long term
- How the contractor will notify the PM of any Hardware needed for sustainment
- Planning for COTS/GOTS usage, commercial capabilities, with impacts of new or changed components
- Planning to minimize the hardware impacts on the business process and the overall enterprise architecture
- Planning phase-out of old equipment
- Planning for consolidation of hardware architecture at a Government designated location
- How the contractor shall analyze and evaluate products for potential employment within the legacy application services
- How the contractor shall use GFE hardware and / or infrastructure services (e.g., cloud services) to accomplish engineering and integration activities
- How the contractor shall engineer hardware changes to meet and align with technology evolution, changes to existing components, and replacement of aged or failed components. Primarily this shall focus on changes to servers and the server farm, but it may also include other areas of the system such as upgrades to end user monitors and viewing devices and integration with overarching changes defined by Air Staff (e.g., centralized server). In designing changes to maintain compliance, to applicable standards and guides, or modernization, the contractor shall leverage and maintain existing legacy information systems architecture as a first choice. Required OV & SV documents or other documentation shall be published IAW the Hardware Sustainment Plan

- How the contractor shall test COTS hardware or supporting components. This shall include test plans, test procedures, and expected test results prepared and submitted for COR approval prior to every hardware release. The test plan, test procedure, and test reports shall be published and coordinated IAW the Hardware Sustainment Plan
- How the contractor shall deploy hardware or supporting components in support of ADLS maintenance release. A VDD shall summarize the results of the delivery to the government. The contractor shall leverage and maintain existing Interface Control Agreements (ICAs) and Interface Control Documents (ICDs) whenever possible and also propose new ICAs/ICDs when needed. The documents shall be stored in a government prescribed location
- How the contractor shall monitor and/or facilitate corrective actions and/or maintenance of these components using the existing maintenance warrantees
- How the contractor shall monitor and support the maintenance of supporting hardware (e.g., power/recoverable, HVAC, hardware and/or rack mounting compliance housing these components)
- How the contractor shall plan, execute and manage the backup of all data.

3.1.3. Compliance Certification

The contractor shall support HQ AETC/A5T completion of legacy information systems National Defense Authorization Act (NDAA) Compliance Certification Package, to include entry of all data into the IT Investment Portfolio Suite (ITIPS), and related compliance systems. Tasks include:

- Application of new/changed guidance requirements provided by the government to update and maintain Enterprise Mission Assurance Support Service (eMASS) compliance packages (Business Management Modernization Program [BMMP], Enterprise Transition Plan [ETP], NDAA and others as required by Air Staff tasking). For example, the kind of information contained in the Capital Investment Report (CIR) and certification packages includes but is not limited to:
    - Business Enterprise Architecture compliance ○ Net-centric compliance ○ Clinger-Cohen Act compliance ○ Privacy Impact Analysis (PIA)
    - 508 Compliance (Section 508 Amendment to the Rehabilitation Act of 1973) ○ System description, stakeholders, Capital Planning and Investment Control (CPIC) status, assumptions
    - Interfaces
    - Relationship to service component reference model ○ Relationship to the technical reference model

  - Enhanced Information Support Plan (EISP), Clinger-Cohen Act (CCA) Compliance Table (AFMAN 17-1402, *Air Force Clinger-Cohen ACT (CCA) Compliance Guide)*, Business Process Reengineering documentation

- Providing Subject Matter Expert (SME) analysis and recommendations as required to AETC A5T
- Update/Maintain ITIPS/eMASS. Given the need for the above information, the contractor shall analyze the above topics and update/maintain ITIPS-related compliance certification packages. This analysis shall include:
  - Conducting program artifact/documentation reviews

eMASS is a government system, the contractor is responsible for entering the legacy information systems security information and artifacts.

3.1.4 Support to Government Leadership

The contractor shall provide information capture/documentation support and Subject Matter Expert (SME) support to the Government, to include Architecture and Data Management Functions, in completing the first two steps of Architecture Development process to determine the intended use, scope, and data required to develop the architecture. The contractor shall provide the technical analyses, expertise, and artifacts necessary to ensure the Government can complete step five of Architecture Development Process.

3.1.5 Configuration Management

The contractor shall accomplish Configuration Management (CM) activities. CM activities include baseline identification, change control, status accounting and auditing.

3.1.6 Configuration Management Plan

The contractor shall provide CM services needed to sustain, integrate, and upgrade capabilities. The contractor shall develop a Configuration Management Plan to serve as the basis for near and long term activities under this work area. Contractor topics in the plan shall include but are not limited to:

- Maintain current and archived software (COTS and custom)
- Coordinate and track progress of system releases
- Administer and maintain Government-provided Serena PVCS Version Manager and Team Track
- Ensure that all tracker items (i.e., change requests, deficiencies) are properly documented and cross referenced to Team Track issues
- How the contractor will manage and prioritize change requests and deficiencies
- Coordinate system builds and installation packages
- Document CM process flows
- Develop and maintain system version documentation
- Coordinate across contractor teams leads (e.g., system administration, database management)
- How the contractor will coordinate with and leverage AETC A5T processes and functions to accomplish the tasks identified in this plan (e.g., coordination with Service Asset and Configuration Management (SACM) for handling of change requests, possible migration to AETC A5T provided ServiceNow suite as the version manager, etc.
- How the CM staff will manage the software and hardware configuration
- How CM will support the tracking and managing new or changes to system components:
  - Manage release notes ○ Equipment phase out

- How CM staff will manage the sustainment releases and sustainment release schedule

- How the Sustainment Release Cycle methodology will be used by the contracting team to sustain through a series of three sustainment releases fielded on a regular schedule throughout the year. The frequency of these three scheduled releases will be scheduled for deployment based on the CCB established fielding schedule. The release cycle will be a set of comprised steps, each with a specific goal that will culminate with the timely release of software changes resulting from user submission of problem reports and change request, plus identified known defects identified as a result of testing and observations.
    - Releases – Releases are updates to the software baseline. They are categorized as: Major, Minor, and Maintenance Releases. The majority of releases follow the normal processes (Plan, Analysis, Design & Build, Test, and finally Deploy). There is no difference in the handling of Major, Minor, and Maintenance Releases. All processes will follow the release schedule that will be coordinated with the Service Manager.
    - Out of Cycle Releases - Contractor will be cognizant of the fact that managing an IT system on the scale of requires flexibility in the event of problems that due to the urgency of the situation cannot wait to be included in the normal releases cycle. In order to accommodate these unique situations, the software sustainment methodology includes provisions for three types of out of cycle releases: Emergency Releases, Patches, and Post-Release Patches. Use of these is limited to specific circumstances, because they could impact the delivery of scheduled releases.
    - NOTE: One type of delivery that is not listed here is Data Fix. A Data Fix does not affect the baseline and therefore has a separate process from releases.
- How CM will support the CCB (report on planned changes, describing way ahead)
- How the contractor will plan, execute and report to the COR on configuration management activities
- How the contractor will manage all of the software and hardware components within the enterprise environment
- How the contractor will manage the software configuration to include evaluation, sustainment, testing, and production components
- How the contractor will manage the hardware configuration to include servers, network devices, and workstations
- How the contractor will manage all current and past system version documentation to include requirements, design and test
- How the contractor will publish release notes for all versions delivered to the user community. Release notes will include a version description (hardware/software change being made configuration specifications).
- How the contractor will document the impact of changes to operational configuration (delivery, transition)

Products and documentation shall be published IAW the Configuration Management Plan

3.1.7. Internal and External Interfaces

The Contractor shall sustain all internal and external interfaces. The contractor shall:

- Plan, schedule, and manage the implementation, sustainment of all legacy information systems COTS/GOTS internal and/or external data interfaces and batch processes in the exact run order specified in each interface description. Run order ensures data between internal and external information systems is current and minimizes rejected updates.

- Continuously examine and evaluate the COTS/GOTS data interface and batch processes, proposing technically feasible improvements to automation that will benefit legacy information systems.
- Capture, troubleshoot, report and resolve COTS/GOTS data interfaces and batch processes for application anomalies or failures.
- Work with internal departments as well as outside activities and agencies diagnosing and resolving problems in response to user reported incidents, customer functional issues, technical problems, questions, or concerns.

Products and documentation shall be published IAW the Database Sustainment and Integration Plan.

3.2 Systems Updates, Migration and Integration

To respond to operational suitability and compliance requirements, system updates shall be necessary. However, these updates shall be limited to the requirements identified in the sub-paragraphs listed below. All systems updates, migration and integration requirements must comply with applicable documents, standards and guides specified in Section 8 of this Task Order PWS.

- Conduct software enhancements, software security, web services development, web services testing, applications and testing, security layer integration, database clean-up, and data conversion.
- Operate and maintain applications, models and databases to determine optimal solutions for integration concepts and problems integral to the integration process. Follow schedules and implementation plans, including parallel operations, identification of technical approaches and a description of anticipated prototype results.
- Perform system performance tuning, system re-hosting and integration services.
- Utilize Government-Off-The-Shelf (GOTS) or approved Commercial-Off-The-Shelf (COTS) tools for systems design and enhancements.

3.2.1. CCB approved updates

The contractor shall provide engineering, software, test, and integration services to deliver system releases IAW the configuration management plan as approved by the COR.

3.3. Information Services

Information services requirements must comply with applicable documents and standards specified in Section 8 of this TO PWS.

3.3.1 Service Lifecycle Management

Generate necessary design and implementation artifacts that shall support life-cycle management, defined as service development, testing, certification, registration, sustainment and evolution aligned with defined requirements. These artifacts shall include the metadata needed for service life-cycle management IAW the current version of the DoD Discovery Metadata Specification (DDMS).

3.3.2 Data Stores

- Create and maintain data stores.
- Provide services such as data cleansing, redundancy resolution and business rule validation.
- Monitor and maintain these data stores to ensure data availability, accuracy, precision and responsiveness.

3.3.3 Information Exposure Services

- Provide application services.
- Prepare and standardize data retrieved from legacy information sources
- Modify the information source’s interface, data and/or behavior for standardized accessibility.
- Transform communication interfaces, data structures and program semantic alignment.
- Provide standardized communication/program wrapping services, data language translation, etc.
- Employ configuration management plan of existing legacy information systems baseline code and data exposure code.

3.4 Systems Operations

Systems operations requirements must comply with applicable documents and standards specified in Section 8 of this TO PWS.

The contractor shall provide operational support services including, but not limited to, database administration, systems administration, and customer training.

3.4.1. Software Analysis and Sustainment

- Ability at expert level to analyze, understand, modify, compile, and deploy complex desktop and web applications
- Provide capability analysis of existing systems.
- Perform security analysis of existing systems and provide appropriate remediation.
- Perform fault and bug assessments and provide and/or recommend appropriate maintenance and security solutions such as patches and hot fixes.
- Assist other software maintenance teams, DBAs, system administrators as directed, authorized, and assigned, by providing results of software/systems analysis.
- Analyze legacy information systems code to identify, fix, or recommend fixes to DBA for bugs caused by improper or incomplete data entry.
- Work with functional and IT teams to compare, evaluate, and test COTS software for potential replacement of legacy system(s).
- Conform to configuration management standards. Properly store baseline code/executables.
- Build awareness of modern software security trends and issues. Make discoveries of potential weaknesses and exploits know to management.
- Transfer software applications to new servers, web servers, and desktop computers and ensure proper operation.

3.4.2 Database Administration

The contractor shall perform the following functions for HQ AETC/A5T Legacy Information Systems in accordance with the approved Database Sustainment and Integration Plan:

- Create and test backups of data, provide data cleansing services, verify data integrity, implement access controls.
- Install and upgrade Oracle server and application tools
- Allocate system storage and plan future storage requirements for the database system.
- Modify/create database storage structures (e.g. tablespaces, tables, views) to support modified application modification.
- Enroll users, grant correct privileges, and maintain correct security settings.
- Ensure compliance with Oracle license agreement.

- Control and monitor user access to the database.
- Monitor and optimize the performance of the database.
- Plan for backup and recovery of database information.
- Maintain archived data on appropriate backup device.
- Provide ability to rapidly restore data and database operations in event of failure.
- Develop, implement, and/or recommend local policies and procedures for security and integrity of databases.
- Resolve database performance and capacity issues, replication, and other distributed data issues.
- Implement and follow industry and government standard database administration concepts, practices, and procedures.
- Troubleshoot and implement virtualized environments.
- Make modest code changes, test, debug, and re-deploy legacy Oracle APEX applications.
- Implement and operate Oracle Automatic Storage Management (ASM).
- Implement and operate Oracle WebLogic.
- Implement Oracle Wallet security measures.
- Transfer Oracle DB and data to new hardware.
- Perform RMAN backups/restores.
- Work closely with security professional to address and fix all security inspection findings.

3.4.2.1. Database Sustainment and Integration Plan

The contractor shall sustain and integrate all legacy information systems databases. The contractor shall develop a Database Sustainment and Integration Plan to serve as the foundation for near and longterm activities under this work area. Contractor topics in the plan shall include but are not limited to:

- How the contractor shall integrate capabilities while sustaining the existing database structure
- How the contractor shall plan, execute and report to the COR on database sustainment and integration activities
- How the contractor shall coordinate with and leverage HQ AETC A5T processes and functions to accomplish the tasks identified in this plan (e.g., coordination with Data & Architecture Function for development of architecture and data artifacts, etc.)
- How the database sustainment and integration work programs shall evolve near and long term
- How the contractor shall manage and test database backup and recovery activities
- Data model management
- Data dictionary and schemas
- What tools are required to ensure consistency and repeatability for database management activities
- Planning for COTS/GOTS usage, commercial capabilities, and EOL migration planning with impacts of new or changed components:
    - ○ Evolutionary impacts of Service-oriented architecture (SOA)
    - ○ Data warehouse ○ Data mining opportunities
- Planning to minimize the database impacts on the business process and the overall enterprise architecture
- Planned database consolidation
- Planned phase-out of old equipment
- How the contractor shall conduct database analysis and performance tuning. Analysis products and recommendations shall be published IAW the Database Sustainment and Integration Plan.

- How the contractor shall maintain multiple databases in support of A5T Legacy Information Systems; at a minimum this shall include database instances for sustainment, training, and production.
- How the contractor shall test database capabilities. This shall include test plans, test procedures, test results prepared and submitted for COR approval prior to every software release. Any test plans, test procedures, and test reports shall be published and coordinated IAW the Software Sustainment Plan.

3.4.3 Systems Administration

The contractor shall sustain HQ AETC/A5T Legacy Information Systems administration capabilities. Systems administration includes all processes necessary to sustain operations on the AFNet. The contractor shall create a Systems Administration Plan to serve as the basis for activities under this area. Contractor topics in the plan shall include but are not limited to:

- Install, support and maintain computer systems.
- Plan and respond to service outages.
- Diagnose software and hardware failures to resolution.
- Implement and ensure security preventive measures are fully functioning.
- Monitor and enhance system performance.
- Manage systems security, and direct and implement the necessary controls and procedures to costeffectively protect information and system assets from intentional or inadvertent modification, disclosure or destruction.
- Manage network security, and direct and implement the necessary controls and procedures to costeffectively protect information and network assets from intentional or inadvertent modification, disclosure or destruction
- Provide system administration of Web and Desktop applications, including administration of user accounts, passwords, email, chat, and File Transfer Protocol (FTP).
- Maintain servers, create monitoring reports and logs, and ensure functionality of links. Monitor web site for acceptable performance and user accessibility. Establish back-ups and monitor site security. Consult with and advise network users concerning network policies, system maintenance and Network accessibility.
- Coordinate network administration and performance requirements with others in the information systems function. Identify, analyze and document long-range requirements and schedule resources related to the enterprise network
- Responsible for configuration management and documentation of network and system topologies and/or web site. Prepare technical implementation plans that provide integrated solutions including actions, milestones, timelines and critical paths required for complete solutions. Timelines and deadlines shall be assigned and provided by the COR and all documentation shall be provided to the COR.
- Research applicable standards and requirements documents to assure compliance. Select or recommend multi-user software that meets common user requirements, integrate (where possible) with existing software. Plan for and provide reasonable responsiveness in terms of system performance.
- Install new software releases, system upgrades, evaluate and install patches and resolve database software related problems.
- Perform system backup and recovery, maintaining data files and monitor system configuration to ensure data integrity.
- Support functional users in troubleshooting computer related problems

- Perform system backup and recovery, maintaining data files and monitors system configuration to ensure data integrity.
- Monitor active web operations to identify performance issues and availability.
- Identify networks outages, firewall issues, bandwidth issues, hardware issues, etc.

3.4.3.1. Systems Administration Plan

The contractor shall sustain the Legacy Information Systems through system administration capabilities. Systems Administration includes all processes necessary to sustain operations on the AFNet. The contractor shall create a Systems Administration Plan to serve as the basis for near- and long-term activities under this work area. Contractor topics in the plan shall include but are not limited to:

- System and data backup (daily)
- Recovery of system and data items as required
- Monitoring system performance (e.g., table or application failures, hardware and network problems, response time by application and/or data)
- Maintain legacy information system Production, Sustainment and Support Servers, operating systems, and communications
- Ensure all systems are scanned and configured IAW Security Technical Implication Guides (STIG) and AF Instructions
- Ensure server security is IAW with local base and AF direction
- Debug errors as they apply to the legacy information systems for all system problems other than COTS Production software
- Maintain commercial support software inventories
- Provide technical support for software configuration and installation procedure definitions
- Create Install Shield installation release packages and field releases
- How the contractor will coordinate with and leverage HQ AETC A5T processes and functions to accomplish the tasks identified in this plan (e.g., coordination with IT Operations Management for submission of firewall change request tickets, etc.)
- How the contractor will facilitate timely repair of COTS hardware products with product vendor
- How the contractor will facilitate timely repair of GOTS/COTS software products
- How the contractor will maintain/update and execute and/or test the COOP plan annually
- How the contractor will coordinate and help facilitate DISA/AFNet network connectivity issues with network personnel (i.e. I-NOSC, MCCC, JBSA-Randolph Communications Squadron) when the legacy information systems encounters network connectivity issues.

- How the contractor will provide Service desk level 1, 2, and 3 problem identification and troubleshooting. Support will encompass software, hardware, and database items/events.
    - Service desk hours are typically 5 days a week, 0730 to 1730. Exceptions will require CO & COR approval.
    - Tier 1 – Basic application software and/or hardware support (e.g., account management, training issue references, basic user support).
    - Tier 2 – More complex support on application software and/or hardware (e.g., HW malfunction, system performance issues, operating system issues, network issues, etc.).
    - Tier 3 – Usually subject matter experts or developer support is required to support complex configuration and/or software issues.

- How the contractor will provide general system information to the community that includes: version release changes, hardware outages, system-wide hardware/software/database problems, authorized service interruptions
- How the contractor will develop, conduct, maintain and/or update student and instructor training programs and materials
- How the contractor will coordinate with and leverage HQ AETC A5T processes and functions to accomplish the tasks identified in this plan (e.g., coordination with Incident Management for handling of tickets, possible migration to the HQ AETC A5T provided ServiceNow suite as the ticketing system, etc.)
- How the contractor will coordinate with users to identify and resolve user problems
- How the contractor will facilitate directing the user to appropriate staff or organization to respond to the problem (e.g., policy issues, hardware configuration, and software failure)
- How the contractor will provide technical support to unit computer managers
- How the contractor will document and manage all trouble ticket problems in the Customer Service Report. The Customer Service Report will provide analysis to support Service desk staffing/manning decisions
- How the contractor will address known database errors
- How the contractor will optimize and sustain a user help content system and professional knowledge bases for legacy information systems.
- How the contractor will manage legacy information systems user accounts and passwords
- How the contractor will provide a known error database to the Service desk

Products and documentation shall be published IAW the Customer Support Plan.

4. ENGINEERING REQUIREMENTS

4.1 Systems Engineering

4.1.1 Life-Cycle Systems Engineering

The contractor shall employ disciplined systems engineering processes including, but not limited to, requirements development, technical management and control, system/software design and architecture, integrated risk management, configuration management, data management, and test, evaluation, verification and validation practices throughout the period of performance of task orders in accordance with AFI 63-1201, *Life Cycle Systems Engineering*.

4.2 Architecture and System Design

The contractor shall support the design and development of systems and applications and their integration into the overarching enterprise architecture IAW the various plans produced under this contract (e.g., Software Sustainment Plan, Hardware Sustainment Plan, etc.). The contractor shall provide the COR all required design and development documents, and supporting architectural documentation IAW the DoD Architecture Framework (DoDAF) version 2.02 identified in this task order IAW Section 8.

4.2.1 Department of Defense Architectural Framework (DoDAF) Guidance

The contractor shall provide all required design and development documents, and supporting architectural documentation in compliance with the latest Department of Defense Architectural Framework (DoDAF) Enterprise Architecture guidance http://dodcio.defense.gov/Portals/0/Documents/DODAF/DoDAF_v2-02_web.pdf.

4.2.2 Federal Desktop Core Configuration (FDCC)

All services provided under this Task Order shall function and be in compliance with the Federal Desktop Core Configuration (FDCC).

4.4 Testing, Reviews, and Audits

The contractor shall conduct testing, product review, and audit requirements IAW the following paragraphs.

4.4.1. Product Testing, Product Review, & Audit Plan

The contractor shall develop a Product Testing, Product Review, & Audit Plan to serve as the basis for near- and long-term activities under this work area. Contractor topics in the plan shall include but are not limited to:

- How the contractor shall comply with HQ AETC A5T testing & audit testing activities, to include regulatory compliance testing, stress test, training test, availability testing, backup and recovery testing, unit testing, system integration testing, regression testing, integration testing, operational testing, initial function, and performance testing. This shall include test planning, test design, test models, test procedures, test scripts, scope of testing. All required testing documentation shall be delivered to the COR 10 duty days prior each system release. The priorities may change from time to time based upon operational considerations, external factors affecting legacy information systems and needs identified by the IPT. Changes shall be identified in the Systems Status Report.
- How the contractor shall coordinate with and leverage HQ AETC A5T processes and functions to accomplish the tasks identified in this plan (e.g., coordination with Service Validation and Testing for conduct of verification tests, etc.)
- How the contractor shall develop scripts and conduct testing for the application, database and operating system IAW test plans.
- How the contractor shall implement the Audit Test Plans and work schedules for legacy information systems activities as published by HQ AETC A5T Service Validation and Testing

4.4.2. Product Testing, Product Review, & Audit Execution

The contractor shall provide product testing, product review, & audit services needed to sustain, integrate, and upgrade the Legacy Information Systems capabilities. These services shall be provided as an autonomous verification and validation (AV&V) function for Legacy Information Systems. In other words, this function does not fall under the direct supervision/management of the contractor's Project Manager. The contractor shall execute the activities identified in the Product Testing, Product Review, & Audit Plan and Quality Control Plan (section 5.20) to include:

- Analyze and evaluate deliveries to ensure quality products and documentation are provided to the COR. All findings shall be reported directly to the COR.
- Conduct autonomous testing of integrated and changed Legacy Information Systems software and components following a test plan and test procedures. Test plans/procedures and test reports shall be delivered directly to the COR.
- Products and documentation shall be published based on procedures provided by HQ AETC A5T Service Validation and Testing

4.5 Cybersecurity Manager/Information Assurance

The contractor shall ensure that all system or application deliverables meet the requirements of DoD and AF Information Assurance (IA) policy. Furthermore, the contractor shall ensure that personnel performing IA activities obtain, and remain current with, required technical and/or management certifications. This acquisition shall provide disciplined systems/specialty engineering and technical support using established government, contractor, and industry processes that encompass the practices and requirements of AETC Technology Integration Division. The contractor shall create Certification and Accreditation (C&A) and Assessment and Authorization (A&A) packages, provide Authority to Operate (ATO) maintenance for the entire range of Information Systems (ISs) necessary for AETC. The contractor shall not perform services that provide inherently Governmental functions. All work performed under this PWS shall be in accordance with (IAW) the Department of Defense Certification and Accreditation Process (DIACAP), or the Risk Management Framework (RMF), as applicable (AETC is currently conducting its A&A process IAW RMF but the shall require ATO maintenance of current DIACAP packages). The contractor shall provide oversight and manage A5T Division Certification and Accreditation (C&A) and Assessment and Authorization (A&A) packages IAW with RMF process. The contractor will ensure RMF process requirements are met; Air Force Instruction (AFI) 17-101, Risk Management Framework (RMF) for Air Force Information Technology (IT); DoDI 8500.01, Cybersecurity, and DoDI 8510.01, Risk Management Framework for DoD Information Technology.

Note: C&A/A&A efforts results in an Authority to Operate (ATO) under DIACAP and the Risk Management Framework (RMF). References and specified directions under this PWS to C&A or A&A imply both processes, and equivalency between them, unless otherwise specified. Hereafter referred to in this PWS as “the authorization process”, also synonymous with the “accreditation process.”

- The contractor shall be familiar with ISSM duties as outlined in DoDI 8500.01 to manage the cybersecurity architecture, requirements, personnel and procedures for the Information System Owner.
- Shall track contracted cybersecurity personnel certification documentation; validate access agreements and compliance with cybersecurity baseline requirements.
- Review documentation to ensure they satisfy Security Engineering and Certification requirements.
- Assist with the review of entered information in the Information Technology Investment Portfolio System (ITIPS) and provide A5T IT Portfolio Management functions.
- Coordinate security-related activities with information security architects, other ISOs, SCA, SCAR, WCO and AO.
- Track Cyber Tasking Orders and provide status for all assigned systems. (See PWS Assigned Systems Attachment 2.)
- Ensure systems are deployed and operated IAW approved system security plan.
- Assess and guide the quality, completeness of C&A, A&A activities, tasks, and resulting artifacts under DIACAP and RMF.

4.5.1 System IA

For those solutions that shall not inherit existing network security controls, and thus integrate an entirely new application system consisting of a combination of hardware, firmware and software, system security assurance is required at all layers of the TCP/IP DoD Model. The contractor shall ensure that all system deliverables comply with DoD and AF IA policy, specifically DoDI 8500.2, *Information Assurance*

Implementation, and AFI 33-200, *Information Assurance Management*. To ensure that IA policy is implemented correctly on systems, contractors shall ensure compliance with DoD and AF Certification & Accreditation policy, specifically DoDI 8510.01, *DoD Information Assurance Certification and Accreditation Process (DIACAP)*, and AFI 17-101, *Risk Management Framework for Air Force Information Technology*. The contractor shall also support activities and meet the requirements of DoDI 8520.02, *Public Key Infrastructure (PKI) and Public Key (PK) Enabling,* in order to achieve standardized, PKI-supported capabilities for biometrics, digital signatures, encryption, identification and authentication.

- The contractor shall provide ISSO functions for the legacy information systems IAW DODI 8500.01, AFI 33-200 and AFI 33-210 for all IA support services to include:

- The contractor shall provide initial authorization package creation and ATO maintenance support. The contractor shall fulfill assignments IAW the framework of DIACAP/RMF to assess and authorize new ISs, and re-authorize existing system maintenance packages for the ISs identified in Table 1. Preparation documents include, but are not limited to:
  - Authority to Test (ATT) ○ Authority to Operate (ATO) ○ Authority to Connect (ATC) ○ Mission Impact Memorandum (MIM) ○ Plan of Action and Milestones (POAM) ○ Program Protection Plan (PPP)
  - System Security Authorization Agreement (SSAA) ○ System Security Plan
  - Urgent Interim Authorization Request (UIAR)

- The contractor shall utilize the DIACAP/RMF authorization processes with all C&A/A&A work. C&A/A&A work performed shall utilize the DIACAP or RMF processes, as directed by the COR. It is important to note that DIACAP is expected to be phased-out in its entirety, and transition entirely to RMF, during the execution of this contract. All package authorizations shall be processed as RMF packages.

- The contractor shall be provided accounts to access and utilize the Enterprise Mission Assurance Support Service (eMASS) and fulfill the Information System Owner (ISO) and ISSE roles in eMASS throughout the authorization process for package creation and reauthorization purposes.

Package Creation:

- The contractor shall create all RMF authorization package documentation artifacts as necessary and in addition to more specific requirements imposed by cognizant authorizing official, or other approving authorities, The contractor shall:
- Develop and update artifacts including but not limited to System Categorization Forms, PIT Designation and Accessibility Level determination Forms, Security Plans (SP), Security Assessment Plans (SAP), Security Assessment Reports (SAR), Privacy Impact Assessments (PIA), Plans of Actions and Milestones (POAM), Risk Assessment Reports (RAR), System Level Continuous Monitoring Strategy (SLCM), Information Security Continuous Monitoring Strategy (ISCM).

- Conduct and interpret automated scan reviews; perform and interpret automated scanning tools.
- Analyze, remediate and document vulnerabilities by: a) Performing vulnerability analysis, b) remediate vulnerabilities posing a corresponding risk to operations (e.g., remove or quarantine), and c) document residual risks into POAMs. It is important to note that this process shall not be relegated to merely passing all vulnerabilities through to POAMs annotation without a specific effort at remediation;
- Scan for and apply remediation in accordance with Defense Information Security Agency (DISA) Security Technical Implementation Guides (STIGs), Security Requirements Guides (SRG), Security Readiness Review (SRR) tools, and generate DISA checklists and/or artifacts.
- Security Compliance shall be required for vulnerability scanning of the ISs. The Government shall provide appropriate access. The contractor is not expected to provide any scanning tools or software licenses for this contract. Contractor scans shall either include full authorization boundaries or include sampling of authorization boundaries as directed by the Contracting Officer's Representative (COR).
- Prepare ISs for the authorization process by making them compliant within the timeframe prescribed by the Information System Security Manager (ISSM) and/or Information System Owner. The contractor shall patch system assets to then-current acceptable levels within the same timeframe. The contractor shall provide additional artifacts to complete authorization and packages based on each package's unique requirement.
- The contractor shall track package creation progress and coordinate among multiple contractors.

ATO Maintenance

- The contractor shall perform ATO maintenance for all DIACAP and RMF authorization packages and create and document all artifacts as necessary and in addition to more specific requirements imposed by cognizant authorizing official, or other approving authorities. The contractor shall:
- Collaborate with the functional representatives (stakeholder[s]) assigned responsibility for the efficacy and operation of that system, as well as those other stakeholders having a vested interest in that system authorization (e.g., ISSE and the ISO equivalents).
- Maintain the IS artifacts, update artifacts based on change management and reporting required by DOD, SAF/CIO, and eMASS.
- Perform all requirements to prepare ISs for the re-authorization process by making them compliant within the timeframe prescribed by the cognizant ISSM. Re-authorization requirements include but are not limited to performing ACAS and SCAP scans then patching and/or remediating system assets to then-current acceptable levels within the same timeframe.

  The contractor shall scan for and apply remediation in accordance with Defense Information Security Agency (DISA) Security Technical Implementation Guides (STIGs), Security Requirements Guides (SRG), Security Readiness Review (SRR) tools, and generate DISA checklists and/or artifacts within the same timeframe. The contractor shall provide any additional artifacts to complete authorization and re-authorization packages based on each package's unique requirement;
- Assist the Government with performing Security Impact Assessments of proposed or actual changes to the ISs and their environment of operation then document findings in a Security Impact Assessment Report.
- Assess, document, and report all security controls, including but not limited to technical, management, operational, not applicable, and inherited by, the ISs.
- Perform remediation actions, determined by the ISSM to be appropriate for each IS; they should include STIG/SRG/SRR requirements and/or remediation, SCA assessment remediation, eMASS requirements, security control update and reconciliation. The contractor shall perform POAM

reconciliation of the eMASS POAM as defined by system categorization or by specific ATO requirements.

- Address all conditions in ATO and PIT Risk Assessment (PRA) letters.
- Update the relevant authorization process security documents and artifacts including, but not limited to: The CAP, PIT Designation and Accessibility Level determination Forms, SP, SAP, SAR, PIA, POAM, RAR, SLCM, ISCM, hardware/software lists, network diagrams and POAM based on the results of the continuous monitoring process for all assigned ISs.
- Perform recurring real-time reviews of system artifacts for the accredited ISs as a result of maintenance performed and change management activities.
- Perform an annual review of IACs for the accredited ISs.
- Report the security status of the ISs (including the effectiveness of security controls employed within and inherited by the system) to the Authorizing Official (AO) – *through* the ISSM – and other appropriate organizational officials IAW the monitoring strategy, including, but not limited to, monthly status updates.
- Review the reported security status of the ISs (including the effectiveness of security controls employed within and inherited by the ISs) on an ongoing basis IAW the monitoring strategy to determine whether the risk to operations, organizational assets, individuals, or other organizations remains acceptable.

4.5.2 Application IA

For those solutions that shall be deployed to Infrastructure as a Service (IaaS), Platform as a Service (PaaS) or similar environments, and thus inherit existing network security controls, application security assurance is required at the Application layer of the TCP/IP DoD Model. The contractor shall ensure that all application deliverables adhere to Public Law 111-383, which states the general need for software assurance. Specifically, the contractor shall ensure that all application deliverables comply with the Defense Information Systems Agency (DISA) Application Security & Development Security Technical Implementation Guide (STIG), which includes the need for source code scanning, the DISA Database STIG, and a Web Penetration Test to mitigate vulnerabilities associated with SQL injections, cross-site scripting and buffer overflows. The contractor shall also support activities and meet the requirements of DoDI 8520.02, *Public Key Infrastructure (PKI) and Public Key (PK) Enabling*, in order to achieve standardized, PKI-supported capabilities for biometrics, digital signatures, encryption, identification and authentication.

4.5.3 Personnel IA

In accordance with DoD 8570.01-M, Information Assurance Workforce Improvement Program and AFMAN 17-1303/33-285 Cybersecurity Workforce (CSWF) Improvement Program, contractor personnel performing cybersecurity functions must be designated as a member of the CSWF and meet qualification requirements for their duties. As the CSWF program definition documents noted above are changed, this PWS shall be reviewed for any clarifications required, as resultant in a Technical Instruction (TI), but not automatic supersession of the requirements are implied by this PWS. The cybersecurity functions may include both cybersecurity (CS) baseline certification and operating system (OS)/Computing Environment (CE) certification requirement per the following:

- Key contractor personnel performing CS functions must meet the minimum CS baseline certification prior to performing services under this PWS.

- Baseline Certification – The baseline certification is a security certification and is required for all CSWF members (all Information Assurance Technician [IAT] and Information Assurance Manager [IAM] levels) of the CSWF.

- Continuing Professional Education (CPE) Requirements – As technology continuously advances, nearly all certifications expire or have CPE requirements. Both the baseline certifications and CE certifications may require continuous education. CPE requirements are not a direct contractor cost to the Government. The contractor is responsible for ensuring its personnel meet the qualification requirements for each personnel's position on the contract, and shall not invoice the Government for training, certification tests, or CPE requirements. The COR shall monitor the certification status of each contractor performing work to this TO, and ensure each contractor is/remains qualified to perform such work.

Upon commencement of performance of this PWS, all contractor personnel assigned to an IAM/IAT Level I-III position shall sign the Information System Privileged Access Agreement and Acknowledgement of Responsibilities statement as required by AFMAN33-285, upon contract award. Individual Privileged Access Agreements may be required, dependent of wing security policies.

4.5.3.5. CSWF positions and labor categories are identified in the Personnel Qualifications section below (Section 5). This PWS includes CS functional services for DoD ISs and requires appropriately certified contractor personnel to access DoD ISs to perform duties under this PWS. After contract award, the contractor is responsible for ensuring that the certifications and certification status of all contractor Personnel performing CS functions as described in DoD 8570.01-M, Change 4, Information Assurance Workforce Improvement Program are in compliance with DoD 8570.01-M, Change 4, and are identified, documented, and tracked. Upon request, the contractor is responsible for providing the CS training certification, certification maintenance, and proof of continuing education and/or sustainment training required for its personnel's CS functional responsibilities to the COR.

5. CONTRACTUAL REQUIREMENTS

5.1 Contractors Use of NETCENTS-2 Products Contract N/A

5.2 Place of Performance

The contractor shall perform the requirements of this PWS as required at Randolph AFB and Lackland AFB. The only exception shall be authorized travel for support purposes.

5.3 Normal Hours of Operation

5.3.1. Contractor personnel are on a standard workweek, Monday – Friday, 07:30am – 5:30pm. Flextime and Alternative Work Schedules (AWS) are not authorized. Occasional change of work hours may be required to accommodate extra ordinary training requirements. A shift in work schedule that are mutually beneficial and do not exceed 80 work-hours shall be coordinated through the COR. Contract work hours shall correspond with Government personnel duty hours.

5.3.2. Holidays. Federal Holidays: HQ AETC follows the established Federal Government schedule for holidays provided during each work year. The holidays recognized by the Federal Government are: New Year's Day, Birthday of Dr. Martin Luther King Jr., Presidents Day, Memorial Day, Independence Day, Labor Day, Columbus Day, Veterans Day, Thanksgiving Day, and Christmas Day. Down-days (i.e., Family Day) declared by the AETC Commander are considered duty days and are not included in the definition of a holiday.

5.4 Government Furnished Property

When this Task Order requires the contractor to work in a Government facility, the Government shall furnish or make available working space, network access and equipment to include: • Windows PC with Microsoft Office Suite (Outlook, Word, Excel, PowerPoint, etc.)

- Telephone (local/long distance calls authorized as dictated by Task Order performance requirements)
- Facsimile
- Copier
- Printer

Copies of required Government furnished materials cited in the solicitation, PWS, DD Form 254, and/or in the Task Order shall be provided to the contractor in hard copy or soft copy. All materials shall remain the property of the Government and shall be returned to the responsible COR upon request or at the end of the Task Order period of performance.

5.5 Billable Hours

In order for man-hours to be billed, deliverable services must have been performed in direct support of a requirement in the TO PWS. In the course of business, situations may arise where Government facilities may not be available for performance of the TO requirements (i.e., base closure due to weather, Force Protection conditions, etc.). When the base is officially closed no contractor services shall be provided and no charges shall be incurred and/or billed to any TO. There may also be occasions when support contractors are invited to participate in morale and recreational activities (i.e., holiday parties, golf outings, sports days and other various social events). Contractor employees shall not be directed to attend such events by the Government. Since a contract employee is not a government employee, the contract employee cannot be granted the same duty time activities as Government employees. Participation in such events is not billable to the TO and contractor employee participation should be IAW the employees' company's policies and compensation system.

5.6 Non-Personal Services

The Government shall 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 (TO) Contracting Officers 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. These operating procedures may be superseded by Theater Commander's direction during deployments.

5.7 Contractor Identification

Contractor personnel shall wear nametags clearly depicting the company and employee's name. All Contractor employees shall identify themselves as Contractors when their status is not readily apparent and display all identification and visitor badges in plain view above the waist at all times. Contractor employees must identify themselves on the phone and in meetings as contract employees. Email addresses and signature blocks must clearly identify them as contractor employees IAW AFI 33-119, paragraph 5.1.5.4.1.7 and Table A2.5. When conversing with Government personnel during business meetings, over the telephone or via electronic mail, contractor/subcontractor personnel shall identify themselves as such to avoid situations arising where sensitive topics might be better discussed solely between Government employees. Contractors/subcontractors shall identify themselves on any attendance sheet or any coordination documents they may review. Electronic mail signature blocks shall identify their company affiliation. Where practicable, contractor/subcontractors occupying collocated space with their Government program customer should identify their work space area with their name and company affiliation. *Refer to Clause H063 of the overarching ID/IQ contract.*

5.8 Performance Reporting

The contractor's task order performance shall be monitored by the Government and reported in Contractor Performance Assessment Reports (CPARs). Performance standards shall include the contractor's ability to provide or satisfy the following:

- Provide satisfactory solutions to requirements with the necessary customer support.
- Provide solutions and services that meet or exceed specified performance parameters.
- Deliver timely and quality deliverables to include accurate reports and responsive proposals.
- Ensure solutions to requirements are in compliance with applicable policy and regulation.

5.9 Program Management/Project Management

The contractor shall identify a Program Manager or a Project Manager who shall be the primary representative responsible for all work awarded under this task order, participating in Program/Project Management Reviews and ensuring all standards referenced herein are adhered to. The contractor shall deliver a Program Management Plan that addresses program management approach, resources, and schedules at a minimum.

5.9.1 Services Delivery Summary

The contractor's performance at the contract level shall be assessed monthly by a process that measures success towards achieving defined performance objectives. The Services Delivery Summary shall be in accordance with AFI 63-101, *Acquisition and Sustainment Life Cycle Management*, AFI 10-601, *Capabilities-Based Requirements Development* and FAR Subpart 37.6, *Performance-Based Acquisition*.

5.9.2 Task Order Management

The contractor shall establish and provide a qualified workforce capable of performing the required tasks. The workforce includes a project manager who will oversee all aspects of the task order. The contractor shall use key performance parameters to monitor work performance, measure results, ensure delivery of contracted product deliverables and solutions, support management and decision-making and facilitate communications. The contractor shall identify risks, resolve problems and verify effectiveness of corrective actions. The contractor shall institute and maintain a process that ensures problems and action items discussed with the Government are tracked through resolution and shall provide timely status reporting. Results of contractor actions taken to improve performance shall be tracked and lessons learned incorporated into applicable processes. The contractor shall establish and maintain a documented set of disciplined, mature and continuously improving processes for administering all contract and Task Order efforts with an emphasis on cost-efficiency, schedule, performance, responsiveness and consistently high quality delivery.

- The Contractor shall provide Project Site Management to manage the contract team and provide programmatic and technical support to HQ AETC A5T in all aspects of the Legacy Information Systems program. The contractor shall manage and direct the activities of sustainment across the contractor team. This will include planning, management, and status reporting.
- The contractor shall perform analysis and planning, and submit technical findings and reports to the Government.
- The contractor shall identify and coordinate all items of work, and assure that all efforts are directed toward a common goal. This program support shall be headed by a Project Manager who shall bear overall responsibility for the successful execution of all work to be performed under this task order. The progress of this effort shall be documented by contractor progress and status reports, briefing materials and milestone reports.
- The contractor shall monitor all performance, attend periodic meetings with Government points of contact; participate in program/project conferences; status reviews; and meetings. The contractor shall provide input, as needed, to the Government regarding the status of all areas of assigned performance to include program status, schedule of milestones, documentation, points of contact, technical issues and action items.
- The contractor shall develop, update and maintain project status briefs, presentation material and milestone charts.
- The contractor shall furnish technical comments and recommendations at program reviews, in process reviews, and technical interchange meetings and provide results in the form of minutes, white papers or technical papers and trip reports.

The contractor shall provide a quarterly Program Management Review (PMR) to the government (CO, COR, and PM). The PMRs will be presented in the form of a PMR Briefing which provides an opportunity for contractor management/team leads (major areas such as Customer Support and Audits) to discuss current efforts, progress, planned activities, and any issues and/or challenges that should be addressed by a joint government/contractor forum. The PMRs will also provide an opportunity for the government to brief their vision on the way ahead and the current status of the Service Delivery. The contractor shall record the results of the PMRs in the PMR Minutes. Minutes will include: contractor/government comments, actions, and guidance/direction and schedule changes.

5.9.3. Key Contractor Personnel Responsibilities

Project Site Management

The contractor shall manage all aspects of software and hardware integration & sustainment, implementation and operations. Key knowledge area requirements include:

- Project planning, resource management, status reporting and priority management (labor applied in support of sustainment and integration)
- Resource management with a diverse labor pool at multiple locations
- Management of military training programs including course development, delivery, student management and reporting
- Military training management operations

Software Sustainment and Integration

The contractor shall sustain large enterprise system components to include adapting COTS/GOTS software. Key knowledge area requirements include:

- Sustainment of learning management or training COTS/GOTS products that are similar to those used by AETC technical training

- Must have expert abilities and strong experience in the following client, server side, IDE, and web technologies:

*WebLogic	Visual Basic 6.0
C#	Access 2007 Visual Basic (VB)
AJAX	Visual Basic for Applications (VBA)
IIS	Java
Object Oriented Principles (OOP)	*Python
.NET 3.5 and .NET 4 Framework	Windows Presentation Foundation (WPF)
Visual Studio 2010-2015	Classic ASP
JavaScript	JQuery
Oracle PL/SQL	Web encryption, authentication, authorization protocols
	Microsoft Team Foundation Server
Test Driven Development (TDD)	Software Configuration Management

Systems Administration

The contractor shall provide systems administration to support information technology projects of this size and complexity. Key knowledge area requirements include:

- Enterprise Engineering (Hardware and Software)
- Virtualization
- VMware Certified Professional on vSphere
- Site surveys
- Product evaluation and testing
- Hardware integration
- AF LAN/WAN design, networks, PKI • Installation, management, and troubleshooting.
- Administering system security systems
- Overseeing LAN/WAN operations pertaining to legacy information systems
- Performing troubleshooting, service calls, and repair of equipment

Database Administration

The contractor shall maintain large databases. Key knowledge area requirements include:

- Ability to develop and implement policies and procedures for ensuring the security and integrity of all databases
- Sustainment and implementation of data models and database designs, data access and table maintenance codes; resolves database performance issues, database capacity issues, replication, and other distributed data issues
- Managing Oracle databases
- Use of standard concepts, practices, and procedures

- Oracle 11g and 12c certifications
- SQL Server and a working knowledge of IIS and/or Apache web server • VMware experience on vSphere

The contractor shall sustain the legacy information systems Virtualization environment

Sustainment Programming

The contractor shall provide programming to maintain the legacy information systems. Key knowledge area requirements include proficiency with the following software:

- Operating Systems: Windows 7, Windows 8, Windows 2008, and Windows 2012 Servers, Red Hat Linux, Solaris 10
- Client/Desktop and web-based using Oracle PL/SQL, Microsoft Visual Basic 6.0, ASP, and ASP.Net - various Microsoft Office 2010, 2013 programs.

Interface Programming

The contractor shall provide interface programming to maintain the Legacy Systems interfaces: A key knowledge area requirement includes:

- Programming in Perl 5.6.1 and web services in .NET using Visual Studio 2013

Configuration Management

The contractor shall perform configuration management of large systems. Key knowledge area requirements include:

- Managing software in a sustainment environment
- Facilitating tracking and management of identified changes in the CCB environment
- Interfacing between the sustainment, government PM, and user community in both an IPT and CCB environment
- Planning, sustainment and maintenance of a Software Engineering Institute (SEI) CMMI level 3

Customer Support

The contractor shall provide customer support to a large legacy systems user population (approximately 760K users). Customer support personnel shall be able to work within a multi-tiered work environment supporting a diverse user community from novice to expert. Key knowledge area requirements include:

- Establishing and operating multi-tiered Service desks
- Resolving problems through disposition
- Managing user accounts
- Assisting users in employing information technologies for defined business processes
- Military training management operations (e.g. Air Force and Army)

Product Testing, Product Review, & Process Audit Services:

The contractor shall prepare Department of Defense A&A package. Key knowledge area requirements include:

- RMF
- A&A processes
- Definition and development of documents needed to obtain a Certification to Operate (CTO) to gain/maintain a Certification of Networthiness (CoN)
- Audit and Test processes
- NDAA process
- AF Architecture
- EISP package

- Software Engineering Institute (SEI) CMMI

Cybersecurity Manager

The Contractor’s personnel will be cybersecurity certified as an Information Assurance Manager Level II or Information Assurance Technical Level III IAW DoDD 8140.01/ DoD 8570.01-M/AFMAN 17-1303.

5.9.4 Documentation and Data Management

The contractor shall establish, maintain and administer an integrated data management system for collection, control, publishing and delivery of all program documents. The data management system shall include but not be limited to the following types of documents: CDRLs, White Papers, Status Reports, Audit Reports, Agendas, Presentation Materials, Minutes, Contract Letters and Task Order Proposals. The contractor shall provide the Government with electronic access to this data, including access to printable reports.

5.9.5 Records, Files, and Documents

All physical records, files, documents and work papers, provided and/or generated by the Government and/or generated for the Government in performance of this PWS, maintained by the contractor which are to be transferred or released to the Government or successor contractor, shall become and remain Government property and shall be maintained and disposed of IAW AFMAN 33-363, Management of Records; AFI 33-364, Records Disposition – Procedures and Responsibilities; the Federal Acquisition Regulation, and/or the Defense Federal Acquisition Regulation Supplement, as applicable. Nothing in this section alters the rights of the Government or the contractor with respect to patents, data rights, copyrights or any other intellectual property or proprietary information as set forth in any other part of this PWS or the Application Services contract of which this PWS is a part (including all clauses that are or shall be included or incorporated by reference into that contract).

5.9.6 Personnel Security

See PWS Security Attachment A

5.9.6 Travel

The contractor shall coordinate specific travel arrangements with the individual Contracting Officer or Contracting Officer’s Representative to obtain advance, written approval for the travel about to be conducted. The contractor’s request for travel shall be in writing and contain the dates, locations and estimated costs of the travel in accordance with the basic contract clause H047.

If any travel arrangements cause additional costs to the task order that exceed those previously negotiated, written approval by CO is required, prior to undertaking such travel. Costs associated with contractor travel shall be in accordance with FAR Part 31.205-46, Travel Costs. The contractor shall travel using the lower cost mode transportation commensurate with the mission requirements. When necessary to use air travel, the contractor shall use economy class or similar accommodations to the extent they are available and commensurate with the mission requirements. Travel shall be reimbursed on a cost reimbursable basis; no profit or fee shall be paid.

5.10 Training

Contractor personnel are required to possess the skills necessary to support their company’s minimum requirements of the labor category under which they are performing. Training necessary to meet minimum requirements shall not be paid for by the Government or charged to TOs by contractors.

5.10.1 Mission-Unique Training

In situations where the Government organization being supported requires some unique level of support because of program/mission-unique needs, then the contractor may directly charge the TO on a cost reimbursable basis. Unique training required for successful support must be specifically authorized by the TO CO. Labor expenses and travel related expenses may be allowed to be billed on a cost reimbursement basis. Tuition/Registration/Book fees (costs) may also be recoverable on a cost reimbursable basis if specifically authorized by the TO CO. The agency requiring the unique support must document the TO file with a signed memorandum that such contemplated labor, travel and costs to be reimbursed by the Government are mission essential and in direct support of unique or special requirements to support the billing of such costs against the TO.

5.10.2 Other Government-Provided Training

The contractor's employees may participate in other Government provided training, on a non-discriminatory basis as among contractors, under the following circumstances:

- The contractor employees' participation is on a space-available basis,
- The contractor employees' participation does not negatively impact performance of this task order,
- The Government incurs no additional cost in providing the training due to the contractor employees' participation, and
- Man-hours spent due to the contractor employees' participation in such training are not invoiced to the task order.

5.11 Data Rights and Non-Commercial Computer Software

In order to implement the provisions at DFARS 252.227-7013(b) and (e) and DFARS 252.227- 7014(b) and (e) and DFARS 252.227-7017, the contractor shall disclose to the ordering Contracting Officer and ordering office in any proposal for a task order, or after award of a task order if not previously disclosed in the proposal, any technical data or non-commercial computer software and computer software/source code documentation developed exclusively at government expense in performance of the task order. This disclosure shall be made whether or not an express requirement for the disclosure is included or not included in the PWS or solicitation for the order. The disclosure shall indicate the rights asserted in the technical data and non-commercial computer software by the contractor and rights that would be acquired by the government if the data or non-commercial software was required to be delivered under the task order and its CDRL requirements and any cost/price associated with delivery. This disclosure requirement also applies to seggragable routines of non-commercial software that may be developed exclusively at Government expense to integrate Commercial Software components or applications provided under a commercial software license or developed to enable Commercial Software to meet requirements of this Task Order. Performance of this disclosure requirement shall be considered a material performance requirement of any task order under which such technical data or non-commercial computer software is developed exclusively at Government expense.

5.12 Software Support and Data Rights

Unless specified otherwise in the Task Order, the contractor shall fully support all unique software developed to support integrated solutions on this contract. The contractor shall be able to support all software revisions deployed or resident on the system and sub-systems. The data rights ownership/licensing guidance is specified in Section I, Clause 252.227-7013 and 252.227-7015 in the overarching contract section B, Defense Federal Acquisition Regulation Supplement Contract Clauses.

5.13 COTS Manuals and Supplemental Data

The contractor shall provide documentation for all systems services delivered under this Task Order. The contractor shall provide COTS manuals, supplemental data for COTS manuals and documentation IAW best commercial practices (i.e. CD-ROM, etc.). This documentation shall include users' manuals, operators' manuals, maintenance manuals and network and application interfaces if specified in the task order.

5.14 Enterprise Software Initiative

In situations where the purchase of new COTS software is needed to satisfy the requirements of a particular task order, the contractor shall use available existing enterprise licenses. If enterprise licenses are unavailable, then products shall be obtained via the DoD Enterprise Software Initiative (ESI) Blanket Purchase Agreements (BPAs). If products are unavailable from ESI, then products shall be acquired through the NETCENTS-2 Products contract. The updated listing of COTS software available from DoD ESI sources can be viewed on the web at: http://www.esi.mil.

5.15 Software License Management

If developing and/or sustaining a system that requires and/or contains COTS, the contractor shall provide maintenance and support of that software license to manage its relationship to the overall system lifecycle in accordance with AFI 33-114, Software Management, which would include applications, license agreements and software upgrades. The contractor shall provide asset inventory and services that track the financial aspects of an asset to include cost and depreciation, contract management, leases, maintenance agreements and service contracts.

The contractor shall provide support summary information to include the general terms and conditions, benefits, strategic and tactical directions, license ordering information, internal billing process, pricing and deployment and support of the products included in the agreement. The contractor shall support common practices for ordering assets, tracking orders and assets and tagging the assets. The contractor shall support application installation, operations, customer support, training, maintenance, and sustainment and configuration control, to include the procurement of supporting software licenses.

5.16 Transition and Decommissioning Plans

The contractor shall create transition and decommissioning plans that accommodate all of the nonauthoritative data sources (non-ADS) interfaces and ensure that necessary capabilities are delivered using approved ADSs.

5.17 Section 508 of the Rehabilitation Act

The contractor shall meet the requirements of the Access Board's regulations at 36 CFR Part 1194, particularly 1194.22, which implements Section 508 of the Rehabilitation Act of 1973, as amended. Section 508 (as amended) of the Rehabilitation Act of 1973 (20 U.S.C. 794d) established comprehensive requirements to ensure: (1) Federal employees with disabilities are able to use information technology to do their jobs, and (2) members of the public with disabilities who are seeking information from Federal sources shall be able to use information technology to access the information on an equal footing with people who do not have disabilities.

5.18 Continuation of Essential Contractor Services during Crisis Declared by the

President of the United States, the Secretary of Defense, or Overseas Combatant Commander

The performance of these services is not considered mission-essential functions during time of crisis. Should a crisis be declared by the Secretary of Defense, the CO or representative shall verbally advise the contractor of the revised requirements, followed by written direction. When a crisis is declared, all services identified in this PWS are considered mission-essential functions during a crisis. The contractor shall continue providing service to the requesting organization 24-hours a day until the crisis is over. The contractor shall ensure enough skilled personnel are available during a crisis for any operational emergency. A crisis management plan shall be submitted IAW A-TE-3, A04, which states that the contractor shall “Submit an essential personnel list within 10 days after the contract start date.” The list shall contain the employee’s name, address, home phone number, beeper number (or cell phone number), social security number, security clearance and duty title. This list shall be updated annually or as changes occur. It must include the language spelled out in DFARS 237.76 – Continuation of Essential Contractor Services to identify services determined mission-essential functions during a crisis situation IAW DODI 3020.37. Note: It is the responsibility of the Combatant Commander to determine mission-essential functions and to establish procedures to ensure that these standard support requirements and any additional requirements are met.

5.19. Special Instructions/Requirements

Personnel Appearance. Contractor personnel shall show clear, continuous evidence of a professional work force. The Contractor’s personnel shall present a neat and well-groomed appearance, and exhibit professionalism. Contractor personnel must wear a badge that clearly indicates that they are Contractor personnel and must have the company logo on it or their apparel. Personnel must clearly identify themselves as contractor employees in emails, over the phone and in meetings. Contractor personnel, although recognized as Contractor employees and under the complete control of the Contractor, shall be required to comply with directives of the base commander or authorized representative as to safety and security standards and regulations applicable to the work site. Contractor personnel involved in crimes and/or other incidents of misconduct may be barred from the base by the base Commander.

Contractor Full-Time Equivalent Reporting. The contractor shall report ALL contractor labor hours (including subcontractor labor hours) required for performance of services provided under this contract for the HQ AETC A5T Legacy Information Systems via a secure data collection site. The contractor is required to completely fill in all required data fields at http://www.ecmra.mil. 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 NLT 31 October of each calendar year. The contractor shall notify the CO when the task is complete.

Uses and Safeguarding Information: Information from the secure web site is considered to be proprietary in nature when the contract number and contractor identity are associated with the direct labor hours and direct labor dollars. At no time will any data be released to the public with the contractor name and contract number associated with the data.

Organizational Conflict of Interest (OCI). IAW FAR 9.505 to prevent conflicting roles that may bias the Contractor's judgment or objectivity, or to preclude the Contractor from obtaining an unfair competitive advantage in concurrent or future acquisitions, the Contractor will be restricted as follows:

- If the Contractor prepares, or assists in preparing, a work statement to be used in competitively acquiring a system or services - or provides material leading directly, predictably, and without delay to such a work statement - the Contractor may not supply the system, major components of the system, or the services unless (a) it is the sole source, (b) has participated in the development and design work or (c) more than one contractor has been involved in preparing the work statement. To overcome the possibility of bias, the Contractor is prohibited from supplying a system or services acquired on the basis of work statements growing out of its services, unless accepted as stated above.

- The Contractor may gain access to proprietary information of other companies during contract performance. The Contractor agrees to enter into company-to-company agreements to (a) protect another company's information from unauthorized use or disclosure for as long as it is considered proprietary by the other company and (b) refrain from using the information for any purpose other than that for which it is furnished. For information purposes, the Contractor shall furnish copies of these agreements to the CO. These agreements are not intended to protect information which is available to the Government or to the Contractor from other sources and furnished voluntarily without restriction.

The above restrictions shall be included in all subcontracts, teaming arrangements, and other agreements calling for performance of work related to this contract, unless excused in writing by the CO.

The above prohibitions do not apply to developmental work, even if the development was funded under a Government contract (see FAR 9.505-2(a)(3)).

5.20. Quality Control Program

Quality Assurance. The government is responsible for inspection/acceptance of all deliverables under this contract. The COR will record all inspection observations. When an observation indicates a defective deliverable, the COR will require the contractor at the site to initial the observation. The initialing of the observation does not constitute concurrence with the observation, only acknowledgment that he or she has been made aware of the defect. COR inspections may occur during the contract performance period on an as needed basis. Such inspections shall be done according to standard inspection procedures or other contract provisions.

Quality Meetings. The CO may require the contractor to meet with the CO, COR, Legacy Systems PM, and other government personnel as deemed necessary. The contractor may request a meeting with the CO when he or she believes such a meeting is necessary. Written minutes of any such meeting will be recorded by the COR and a copy of the minutes will be sent to all attendees. If no response is received within ten calendar days, the minutes shall stand as written. A copy of all recorded minutes will be provided to the contractor, and a copy will be placed in the official contract file for record keeping purposes. In the event the contractor does not concur with any portion of the minutes, exceptions to the minutes shall be provided, in writing, to the CO within ten calendar days following receipt of the minutes. Final resolution to exceptions taken by the contractor resides with the CO.

Quality Control Plan. The contractor shall provide and maintain a current Quality Control Plan (QCP) which shall ensure the requirements of the contract are provided as specified. The QCP will be considered acceptable and approved unless the contractor is notified by the CO prior to award. The QCP shall be submitted as part of the technical proposal for evaluation. Any change to the approved QCP that may become necessary during the life of the contract must be submitted through the COR to the CO for approval prior to any change being affected by the contractor.
Records Inspections. The records of inspections conducted by the contractor shall be kept and made available to the CO or COR throughout the contract performance period and for the period after contract completion until final settlement of any claims under this contract.

Conflict of Interest. The contractor shall not employ any person who is an employee of the US government if employing that person would create a conflict of interest. Additionally, the contractor shall not employ any person who is an employee of the Department of the Air Force, either military or civilian, unless such person seeks and receives approval according to DoD 5500-7-5, *Standards of Conduct*. The contractor shall not employ any person who is an employee of the Department of the Air Force if such employment would be contrary to the policies in AFI 64-106, *Air Force Industrial Labor Relations Activities*. The contractor is cautioned that off-duty active military personnel hired under this contract may be subject to permanent change of station, change in duty hours, or deployment. Military Reservists and National Guard members may be subject to recall to active duty. The abrupt absence of these personnel could adversely affect the contractor's ability to perform; however, their absence at any time shall not constitute an excuse for nonperformance under this contract.

Ownership. All material (e.g., software, documentation, design, concepts) produced and/or delivered by the contractor under this PWS shall become the sole property of the government.

6.   SERVICES DELIVERY SUMMARY

Performance Requirement	Performance Threshold	Monitoring Method
1. Monthly Status Report	COR approval of report with no major revision at 90% of the time	Periodic inspection of deliverable products least
2. CSWC	100% of personnel maintain proper and current certifications to perform assigned functions IAW DoD 8570	100% inspection of personnel certifications
3. Service Sustainment and Enhancements	No more than one (1) unscheduled system outage per quarter due to hardware	Periodic inspection of unscheduled system outage metrics/customer

	or software failure	input
4. Software Maintenance/ Updates/Upgrades and Patches	No more than one software discrepancy reported per 10 software maintenance and enhancement implementation	Periodic inspection
5. System Security	Results of all CAT vulnerabilities and scans will be reported to the COR within 24 hours 95% of system upgrades, patches, and hot fixes are applied within established timelines and POA&Ms created for all that do not get implemented within established timelines.	100% inspection
6. Security Accreditation	Maintain A&A ATO/ATC	100% inspection compliance IAW applicable DoD and AF policy and instruction with no more than three errors in Security Control documentation per package, per quarter due to contractor caused error.
7. RMF A&A Package	No more than one Package Approval Chain (PAC) reject per package for rework due to contractor caused errors.	100% inspection
8. Systems Analysis	No more than 1 analysis error provided per month to customer	100% inspection
9. Database Administration and Programming Support	Maintain development and test environments	Periodic inspection

10. Configuration	Configuration management	Periodic inspection management database

database includes all updates and accuracy	98% accuracy rate is maintained at all times	systems and software and a
11. Product Testing, Product Review and Process Audit Services	Acceptance test of approved system changes will be conducted with zero errors or defects that affect fielding decisions.	Periodic inspection

7. SECURITY REQUIREMENTS

See PWS Security Attachment A

8. DATA DELIVERABLES

A001	DI-CMAN-	Contractor's Configuration Management Plan 80858B
A002	DI-CMAN-80874	Configuration Data Lists (CDLS)
A003	DI-CMAN-81022C	Configuration Audit Summary Report

A004 DI-CMAN-81121 Baseline Description Document A005 DI-

IPSC-80942 Computer Software System Document

A006	DI-IPSC-81427A	Software Development Plan (SDP)
A007	DI-IPSC-81428A	Software Installation Plan (SIP)
A008	DI-IPSC-81429A	Software Transition Plan (STRP)
A009	DI-IPSC-81433A	Software Requirements Specification (SRS)
A010	DI-IPSC-81434A	Interface Requirements Specification (IRS)
A011	DI-IPSC-81435A	Software Design Description (SDD)
A012	DI-IPSC-81436A	Interface Design Description (IDD)
A013	DI-IPSC-81438A	Software Test Plan (STP)
A014	DI-IPSC-81439A	Software Test Description (STD)
A015	DI-IPSC-81440A	Software Test Report (STR)
A016	DI-IPSC-81442A	Software Version Description (SVD)
A017	DI-IPSC-81488	Computer Software Product
A018	DI-IPSC-81756	Software Documentation
A019	DI-MCCR-80902	Software Development Summary Report
A020	DI-MCCR-81344	Design Specification
A021	DI-MGMT-80469A	System Assessment Report (SAR)

A022	DI-MGMT-80501	Contractor's Corrective Action Plan
A023	DI-MGMT-80920	List of Items Delivered During the Term of a Contract
A024	DI-MGMT-	Contract Performance Report (CPR) 81466A
A025	DI-MGMT-81580	Contractor's Standard Operating Procedures
A026	DI-MGMT-81739B	Software Resources Data Reporting: Initial Developer Report and Data Dictionary
A027	DI-MGMT-81740A	Software Resources Data Reporting: Final Developer Report and Data Dictionary
A028	DI-MGMT-81797	Program Management Plan
A029	DI-MGMT-81844	Information Assurance (IA) Test Plan
A030	DI-MISC-80564	Vulnerability Analysis Report
A031	DI-MISC-81807	Software/Firmware Change Request
A032	DI-NUOR-81412	Software Certification Plan (SCP)
A033	DI-QCIC-80736	Quality Deficiency Report
A034	DI-QCIC-81187	Quality Assessment Report
A035	DI-QCIC-81200	Quality Inspection Test, Demonstration, and Evaluation Report
A036	DI-QCIC-81795	Software Quality Assurance Report
A037	DI-RELI-80254	Corrective Action Plan

The Government reserves the right to review all data deliverables for a period of 10 working days prior to acceptance. No data deliverable shall be assumed to be accepted by the Government until the 10-day period has passed, unless the Government explicitly states otherwise in the task order.

The Government requires all deliverables that include Scientific and Technical Information (STINFO), as determined by the Government, be properly marked IAW DoD Directive 5230.24 and AFI 61-204 prior to initial coordination or final delivery. Failure to mark deliverables as instructed by the Government shall result in non-compliance and non-acceptance of the deliverable. The contractor shall include the proper markings on any deliverable deemed STINFO regardless of media type, stage of completeness or method of distribution. Therefore, even draft documents containing STINFO and STINFO sent via e-mail require correct markings. Additionally, as required by individual Task/Delivery Orders, the contractor shall formally deliver as a CDRL all intellectual property, software, licensing, physical records, files, documents, working papers and other data for which the Government shall treat as deliverable.

9. APPLICABLE STANDARDS AND REFERENCES

http://dodcio.defense.gov/ The Department of Defense Architecture

Department of Framework (DoDAF), Version 2.0 is the

TodayinCIO/DoDArchite

Defense overarching, comprehensive framework and

Architecture ctureFramework.aspx conceptual model enabling the development of

Framework architectures to facilitate the ability of

(DoDAF) Ver2.02 Department of Defense (DoD) managers at all Aug 2010 levels to make

key decisions more effectively

through organized information sharing across the Department, Joint Capability Areas (JCAs), Mission, Component, and Program boundaries. The DoDAF serves as one of the principal pillars supporting the DoD Chief Information Officer (CIO) in his responsibilities for development and maintenance of architectures required under the Clinger-Cohen Act. DoDAF is prescribed for the use and development of Architectural Descriptions in the Department. It also provides extensive guidance on the development of

		architectures supporting the adoption and execution of Net-centric services within the
AFI 63-101, Integrated Life Cycle Management	http://static.e-publishing.af.mil/production/1/saf_aq/publication/afi63-101_20-101/afi63-101_20-101.pdf	The purpose of this instruction is to implement direction from the Secretary of the Air Force as outlined in Air Force Policy Directive (AFPD) 63-1/20-1, Acquisition and Sustainment Life Cycle Management. The primary mission of the Integrated Life Cycle Management (ILCM) Enterprise is to provide seamless governance, transparency and integration of all aspects of weapons systems acquisition and sustainment management.
Industry Best Practices in Achieving Service Oriented Architecture (SOA)	http://www.sei.cmu.edu/library/assets/soabest.pdf	This document was developed under the Net-Centric Operations Industry Forum charter to provide industry advisory services to the Department of Defense (DoD), Chief Information Officer (CIO). It presents a list of industry best practices in achieving Service Oriented Architecture (SOA).
DoDI 8500.01 Cybersecurity	http://www.dtic.mil/whs/directives/corres/pdf/850001_2014.pdf	Establishes policy and assigns responsibilities to achieve Department of Defense (DoD) Information Assurance (IA) through a defense-in-depth approach that integrates the capabilities of personnel, operations, and technology, and supports the evolution to network centric warfare.
DoD 8570.01, Information Assurance Training, Certification, and Workforce Management	http://www.dtic.mil/whs/directives/corres/pdf/857001p.pdf	Establishes policy and assigns responsibilities for Department of Defense (DoD) Information Assurance (IA) training, certification, and workforce management.

DoD 8570.01-M, Information Assurance Workforce Improvement Program	http://www.dtic.mil/whs/ directives/corres/pdf/8570 01m.pdf	Provides guidance for the identification and categorization of positions and certification of personnel conducting Information Assurance (IA) functions within the DoD workforce supporting the DoD Global Information Grid (GIG) per DoD Instruction 8500.2. The DoD IA Workforce includes, but is not limited to, all individuals performing any of the IA functions described in this Manual. Additional chapters focusing on personnel performing specialized IA functions
DoDI 8510.01,Risk Management Framework (RMF) for DoD Information Technology (IT)	http://www.dtic.mil/whs/ directives/corres/pdf/8510 01_2014.pdf	Provides procedural guidance for the reciprocal acceptance of authorization decisions and artifacts within DoD, and between DoD and other federal agencies, for the authorization and connection of information systems (ISs).

AFI 33-200, Information Assurance	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afi33-210/afi33-210.pdf	This AFI provides general direction for implementation of IA and management of IA programs according to AFPD 33-2. Compliance ensures appropriate measures are taken to ensure the availability, integrity, and confidentiality of Air Force ISs and the information they process.
Security Technical Implementation Guides (STIGs)	http://iase.disa.mil/stigs/Pages/index.aspx	The Security Technical Implementation Guides (STIGs) and the NSA Guides are the configuration standards for DOD IA and IA-enabled devices/systems. The STIGs contain technical guidance to "lock down" information systems/software that might otherwise be vulnerable to a malicious computer attack.
Federal Information Security Management Act (FISMA) 2002	http://www.dhs.gov/federal-information-security-management-act-fisma	FISMA was enacted as part of the E-Government Act of 2002 to “provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets,” and also to “provide for development and maintenance of minimum controls required to protect Federal information and information systems.”
ISO/IEC 19770-2, Software Tagging	http://www.iso.org/iso/catalogue_detail.htm?csnumber=53670	ISO/IEC 19770-2:2009 establishes specifications for tagging software to optimize its identification and management.
DoDD 8320.1 Data	https://acc.dau.mil/adl/en-	This Instruction applies to the administration and standardization of DoD standard data elements

Administration	US/33650/file/6823/DoD D83201%20Data%20Ad min.pdf	generated within the functional areas of audit and criminal investigations for DoD. It also applies to the administration of DoD standard and nonstandard data elements generated, stored, or used by the DoD. Data elements shall be administered in ways that provide accurate, reliable, and easily accessible data throughout the DoD, while minimizing cost and redundancy. Data elements

10. PRODUCTS STANDARDS AND COMPLIANCE REQUIREMENTS

10.1 Information Assurance (IA) Technical Considerations

The contractor shall recommend Commercial-Off-The-Shelf (COTS) IA and IA-enabled products IAW AFI 33-200, Information Assurance. These products must be Committee on National Systems Security Policy Number 11 (CNSSP-11) compliant, requiring them to be validated by accredited labs under the National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme or National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) Cryptographic Module Validation Program (CMVP). The following are some examples of IA and IA enabled devices: data/network encryptors, intrusion detection devices such as Firewalls, Intrusion Detection System, Authentication Servers, Security Gateways, High Assurance IP encryptor and Virtual Private Networks.

10.2 DoD IPV6 Requirement

All Recommended Products must meet the criteria in DoD IPv6 Standard Profiles for IPv6 Capable Products version 5.0 July 2010 (http://jitc.fhu.disa.mil/apl/ipv6/pdf/disr_ipv6_50.pdf). Some example IPV6 mandated products from the DoD IPV6 Standards Profile are listed below:

- Host/Workstations - a desktop or other end-user computer or workstations running a general purpose operating system such as UNIX, Linux, Windows or a proprietary operations system that is capable of supporting multiple applications.
- Network Appliance or Simple Server - Simple end nodes such as cameras, sensors, automation controllers, networked phones or adapters such as Circuit-to-Packet (CTP) devices, typically with an embedded operating system and specialized software for limited applications. A Network Appliance is typically managed by an end-user, but may support more than one concurrent user remotely via a Web browser interface. A Simple Server supports a small number of concurrent clients via a web browser interface or other protocol with a client application. Examples of simple servers are stand-alone network print servers, storage servers, Session Initiation Protocol (SIP)11 servers, a “web camera” appliance that serves pictures via an embedded web server and a network time server appliance that solely functions to serve NTP requests. Advanced Server - End Nodes with one or more server-side applications (for example Dynamic Host Configuration Protocol (DHCPv6), Domain Name Server (DNS), Network Time Protocol (NTP), E-mail, File Transfer

Protocol (FTP), Hypertext Transfer Protocol (HTTP), web server, storage server or database) to support clients in the network.

- Intermediate Nodes – routers, switches, IA or IA enabled devices.

- IPV6 Capable Software - a product that implements functions available via an IPv6 interface to end-users, network nodes or other software, when installed on an appropriate hardware platform.

10.3 Energy Star

All applicable Products must be EnergyStar® compliant per DoDI 4170.11 and FAR Part 52.223153.

ENERGY EFFICIENCY IN ENERGY-CONSUMING PRODUCTS (DEC 2007)

(a) Definition: As used in this clause, "Energy-efficient product"…

(1) Means a product that—

(i) Meets Department of Energy and Environmental Protection Agency criteria for use of the Energy Star® trademark label; or

(ii) Is in the upper 25 percent of efficiency for all similar products as designated by the Department of Energy's Federal Energy Management Program.

(2) The term "product" does not include any energy-consuming product or system designed or procured for combat or combat-related missions (42 U.S.C. 8259b).

(b) The Contractor shall ensure that energy-consuming products are energy efficient products i.e., ENERGY STAR products or FEMP-designated products) at the time of contract award, for products that are—

(1) Delivered;

(2) Acquired by the Contractor for use in performing services at a Federally-controlled facility;

(3) Furnished by the Contractor for use by the Government; or

(4) Specified in the design of a building or work, or incorporated during its construction, renovation, or maintenance.

(c) The requirements of paragraph (b) apply to the Contractor (including any subcontractor) unless—

(1) The energy-consuming product is not listed in the ENERGY STAR Program or FEMP; or

(2) Otherwise approved in writing by the Contracting Officer.

(d) Information about these products is available for—

(1) ENERGY STAR at http://www.energystar.gov/products; and

(2) FEMP at www.femp.energy.gov/technologies/eep_purchasingspecs.html.

NOTE: Remove if not applicable. The following are some example products that are required to be energy star compliant: computers, displays and monitors, enterprise servers, copiers, digital duplicators, fax/printer machines, printers, scanners, televisions, cordless phones, battery chargers, set-top and cable boxes, and audio and video equipment. For further guidance please see the below URL: http://www1.eere.energy.gov/femp/technologies/eep_purchasingspecs.html

10.4 Encryption Mandates

All Recommended Products that shall perform any type of data encryption, it is required that the encryption method being used meets FIPS standards for both information assurance and interoperability testing. For more information on FIPS, go to: http://www.itl.nist.gov/fipspubs/by-num.htm. Some example FIPS standards would be FIPS 201 which specifies the architecture and technical requirements for a common identifications standard for Federal employees and contractors (i.e. Common Access Card). Another one is FIPS 140-2 which specifies the security requirements that shall be satisfied by a cryptographic module (i.e. the underlying algorithms to process information).

10.5 BIOS Mandate

All Products shall be BIOS protection compliant with Section 3.1 "Security Guidelines for System BIOS Implementations of SP 800-147," per DoD CIO, in order to prevent the unauthorized modification of BIOS firmware on computer systems.

10.6 Biometric Mandate

All Biometric products shall be built to the DoD Electronic Biometric Transmission Specification (EBTS) version 3.0 standard. For more information please visit the Biometric Identity Management Agency website at: http://www.biometrics.dod.mil/.

10.7 Special Asset Tagging

The contractor shall provide special asset tags IAW DODI 8320.04, Item Unique Identification (IUID) Standards for Tangible Personal Property, to Include Unique Identification (UID) tagging requested by non-DoD customers. NOTE: Remove if not applicable. If the following criteria apply then leave the above statement in your PWS. All items for which the Government's unit acquisition cost is $5,000 or more;

- Items for which the Government's unit acquisition cost is less than $5,000, when identified by the requiring activity as DoD serially managed, mission essential or controlled inventory.

- When the Government's unit acquisition cost is less than $5,000 and the requiring activity determines that permanent identification is required.

- Regardless of value, (a) any DoD serially managed subassembly, component or part embedded within an item and, (b) the parent item that contains the embedded subassembly, component or part.

If you require further guidance on Special Asset Tagging please see DoDI 8320.04 at: http://www.dtic.mil/whs/directives/corres/pdf/832004p.pdf.

10.8 Software Tagging

Commercial off-the-shelf software items shall support International Standard for Software Tagging and Identification, ISO/IEC 19770-2, Software Tags when designated as mandatory by the standard. NOTE: Check ISO/IEC 19770-2 to see if Software Tagging applies to this acquisition. Some examples of when you might require software tagging would be if you needed to record unique information about an installed software application or to support software inventory and asset management. For more information please go to: http://tagvault.org/.

10.9 Radio Frequency Identification (RFID)

The contractor shall provide RFID tagging IAW DoD Radio Frequency Identification (RFID) Policy, 30 July 2004 or most current version. NOTE: Check RFID Policy, 30 July 2004 at: https://acc.dau.mil/adl/en- S/142796/file/27748/ RFIDPolicy07-30-2004.pdf to see if Special Asset Tagging applies to this acquisition. Some example uses of RFID are when tags are placed into freights containers, ammunition shipments or attached to unit level IT equipment to facilitate accountability.

10.10 Hardware and Associated Software and Peripherals

Hardware will not be delivered under this DO.

10.11 Authorized Resellers N/A.

10.12 Technical Refresh

In order to ensure new design enhancements and technological updates or advances, the contractor shall offer, under this DO, hardware and software components available to the contractor's commercial customers. Furthermore, the contractor shall make available any commercially available updates to the hardware and software provided under this DO. If such updates are available to other customers without charge, then they shall also be made available to the Government without additional charge. The contractor shall ship these updates to existing customers who have acquired the hardware/software being updated under this DO. Vendor commercial product offerings shall include “state of the art” technology, i.e., the most current proven level of development available in each product category.

10.13 Trade Agreement Act (TAA)

All proposed products must be compliant with the Trade Agreements Act of 1979 (TAA) and related clauses in Section I of this contract. In accordance with DFARS 252.225-7021, the Trade Agreements Certificate at DFARS 252.225-7020 shall be provided for each end item defined and specified in a solicitation that exceeds the TAA threshold subject to the waivers and exceptions provided in FAR 25.4, and DFARS 225.4 offered in response to any RFQ issued under this contract. Please note that Federal Acquisition Regulation (FAR) paragraph 25.103(e) includes an exemption from the Buy American Act (BAA) for acquisition of information technology that are commercial items.

Attachment A Security

1. *Visitor Group Security Agreement (VGSA).* The contractor shall enter into a long-term visitor group security agreement if service performance is on base. This agreement shall outline how the contractor integrates security requirements for service operations with the Air Force to ensure effective and economical operation on the installation. The agreement shall include:

a. Security support provided by the Air Force to the contractor shall include storage containers for classified information/material, use of base destruction facilities, classified reproduction facilities, use of base classified mail services, security badging, base visitor control, investigation of security incidents, base traffic regulations and the use of security forms and conducting inspections required by DoD 5220.22-R, *Industrial Security Regulation,* Air Force Policy Directive 16-14, *Security Enterprise Governance,* and Air Force Instruction 16-1406, *Air Force Industrial Security Program.*

b. Security support requiring joint Air Force and contractor coordination includes packaging classified information, mailing and receiving classified materials, implementing emergency procedures for protection of classified information, security checks and internal security controls for protection of classified material and high-value pilferable property.

c. On base, the long-term visitor group security agreement may take the place of a *Standard Practice Procedure* (SPP).

2. ***Obtaining and Retrieving Identification Media.*** As prescribed by the AFFAR 5352.242-9000, *Contractor access to Air Force installations*, the contractor shall comply with the following requirements:

a. The contractor shall obtain installation access passes for all contractor personnel who make frequent visits to or perform work on the Air Force installation(s) cited in the contract. Contractor personnel are required to present the installation access pass while visiting or performing work on the installation.

b. No later than ten working days prior to contract commencement, the contractor shall submit a written request on company letterhead to the contracting officer, listing the following: contract number, location of work site, start and stop dates, and names, dates of birth, driver’s license number and state of issue for the contractor employees needing access to the base. The authorized security manager will endorse the request and forward it to the issuing installation pass and registration office or security forces for processing. Contractors will present government (state or federal) issued ID, before being issued a pass to enter the installation. Before being issued a pass to enter the installation, a criminal history check will be conducted for every individual requesting a pass. Personnel employed by the contractor and operating a motor vehicle on the installation must possess proof of the following:

(1) Liability Insurance
(2) Current License Plates
(3) Current State Inspection Sticker (If Required)
(4) Valid State Driver License
(5) A phone number for sponsor on base

c. Vehicles owned by the contractor with the company name permanently printed on them are not required to obtain a pass as long as a current work order is presented at the time of entry. However, current liability insurance, state inspection sticker, and registration is required. The person driving the vehicle must have a valid operator license for the type of vehicle.

d. Upon completion or termination of the contract or expiration of the identification passes, the contractor shall ensure that all base identification credentials issued to contractor employees are returned to the issuing office. If a contractor employee has been terminated, the credentials will need to be retrieved and returned to issuing activity so that employee does not have base access. If the credential is not retrieved then SF will need to be notified so base access is not allowed.

e. Failure to comply with these requirements may result in withholding of final payment.

3. ***Pass and Identification Items.*** The contractor shall ensure the following pass and identification items required for service performance are obtained for employees and non-government owned vehicles:

a. Installation Access Pass (IAP) (DBIDS), Visitor/Vehicle Pass (AFMAN 31-116), used for contracts for less than six months to include one-day visits (i.e. warranty work).

b. Installation Access Card (IAC) (DBIDS), (AFMAN 31-113), used for contracts for more than six months or more.

c. DoD Common Access Card (CAC), (AFI 36-3026), used for contracts for more than six months and requirement exists for access to the government computer systems and software. CAC applications are accomplished by Trusted Agents via the Trusted Agent Sponsorship System (TASS).

4. ***Security Clearance Requirements.*** The contractor does not require access to classified information and does not require a facility security clearance.

5. ***List of Employees.*** The contractor shall maintain a current list of employees. The list shall include employee's name, social security number, and level of security clearance. The list shall be validated and signed by the company *Facility Security Officer* (FSO) and provided to the contracting officer and *Information Protection Office* (IP Office) at each performance site 30 days prior to the service start date. Updated listings shall be provided when an employee's status or information changes. A Visit Request for all employees with a security clearance is required to be sent through the Joint Personnel Adjudication System (JPAS), and must be updated at least annually. The contractor shall notify the Information Protection Office at each operating location 30 days before on-base performance of the service. The notification shall include:

a. Name, address, and telephone number of company key management representatives.

b. The contract number and contracting agency.

c. The highest level of classified information to which employees require access.

d. The location(s) of service performance and future performance, if known.

e. The date service performance begins.

f. Any change to information previously provided under this paragraph.

6. ***Suitability Investigations.*** Contractor personnel not requiring access to classified shall successfully complete, as a minimum, a Tier 1 (T1) investigation, before operating government furnished workstations. The contractor shall comply with the DoD 5200.2-R, *Personnel Security Program*, AFMAN 33-152, *User Responsibilities and Guidance for Information Systems*, and AFI 33-200, *Information Assurance (IA) Management*, requirements. T1 investigation requests are initiated using the Standard Form (SF) 85 and are submitted to the installation Information Protection Office through the using agency's Unit Security Manager. T1 investigations are different from the Wants and Warrants checks, and are provided by the government at no additional cost to the contractor.

7. ***Security Monitor Appointment.*** The contractor shall appoint a security representative for the on base long term visitor group. The security representative may be a full-time position or an additional duty position. The security representative shall work with the host organization to provide employees with training required by DoDM 5200.01, *Information Security Program*, AFPD 16-14, *Security Enterprise Governance*, and AFI 16-1404, Air *Force Information Security Program*. The contractor shall provide initial and follow-on training to contractor personnel who work in Air Force controlled/restricted areas. Air Force restricted and controlled areas are explained in AFI 31101, *Integrated Defense*.

8. ***Additional Security Requirements.*** In accordance with DoDM 5200.01, *Information Security Program* and AFI 16-1404, the contractor shall comply with AFSSI 7700, *Emission Security* (EMSEC) Program; applicable AFKAGs, AFIs, and AFSSIs for Communication Security (COMSEC); and AFI 10-701, *Operations Security (OPSEC) Instructions*. The contractor will comply with DoD Standard 22/Force Protection Condition Measures, DoD Standard 25/Level I-AT Awareness Training, and associated tasking contained in AFI 10-245, Antiterrorism (AT) standards. Level I AT Awareness training is available for contractor personnel and can be requested by calling the local installation AT Office.

9. ***Freedom of Information Act Program (FOIA).*** The contractor shall comply with DoD Regulation 5400.7-R/Air Force Supplement, *DoD Freedom of Information Act Program*, requirements. The regulation sets policy and procedures for the disclosure of records to the public and for marking, handling, transmitting, and safeguarding *For Official Use Only (FOUO)* material. The contractor shall comply with AFI 33-332, *Privacy Act Program*, when collecting and maintaining information protected by the Privacy Act of 1974 authorized by Title 10, United States Code, Section 8013. The contractor shall remove or destroy official records only in accordance with AFI 33-322 *Records Management*, or other directives authorized in AFI 33-364, *Records Disposition—Procedures and Responsibilities*.

10. ***Reporting Requirements.*** The contractor shall comply with AFI 71-101, Volume- 1, *Criminal Investigations,* and Volume-2, *Protective Service Matters,* requirements. Contractor personnel shall report to an appropriate authority, any information or circumstances of which they are aware may pose a threat to the security of DoD personnel, contractor personnel, resources, and classified or unclassified defense information. Contractor employees shall be briefed by their immediate supervisor upon initial on-base assignment and as required thereafter.

11. ***Physical Security.*** Areas controlled by contractor employees shall comply with base Operations Plans/instructions for FPCON procedures, Random Antiterrorism Measures (RAMS) and local search/identification requirements. The contractor shall safeguard all government property, including controlled forms, provided for contractor use. At the close of each work period, government training equipment, ground aerospace vehicles, facilities, support equipment, and other valuable materials shall be secured. During increased FPCONs, contractors may have limited access to the installation and should expect entrance delays.

12. ***Operating Instructions***. For controlled areas used exclusively by the contractor, the contractor shall develop an Operating Instruction (OI) for internal circulation control, protection of resources and to regulate entry into Air Force controlled areas during normal, simulated and actual emergency operations. The OI shall be written in accordance with AFI 31-101, the local base Operations Plan usually referred to as an OPLAN and AFI 10-245, *Air Force Antiterrorism (AT) Standards,* and coordinated through the Information Protection (IP) office.

13. ***Key Control.*** The contractor shall establish and implement key control procedures in the Quality Control Plan to ensure keys issued to the contractor by the government are properly safeguarded and not used by unauthorized personnel. The contractor shall not duplicate keys issued by the government. Lost keys shall be reported immediately to the contracting officer. The government replaces lost keys or performs re-keying. The total cost of lost keys, re-keying or lock replacement shall be deducted from the monthly payment due to the contractor. The contractor shall ensure its employees do not allow government issued keys to be used by personnel other than current authorized contractor employees. Contractor employees shall not use keys to open work areas for personnel other than contractor employees engaged in performance of duties, unless authorized by the government functional area chief.

14. ***Lock Combinations.*** The contractor shall establish procedures in local OIs ensuring lock combinations are not revealed to unauthorized persons and ensure the procedures are implemented. The contractor is not authorized to record lock combinations without written approval by the government functional area chief. Records with written combinations to authorized secure storage containers or Secure Storage Rooms (SSR), shall be marked and safeguarded at the highest classification level as the classified material maintained inside the approved containers. The contractor shall comply with DoDM 5200.01, Vol 3 security requirements for changing combinations to storage containers used to maintain classified materials.

15. ***Traffic Laws.*** The contractor and their employees shall comply with base traffic regulations.

16. ***Healthcare.*** Healthcare provided at the local military treatment facility on an emergency reimbursable basis only.