Air Force Personnel Activity
Information Technology (IT) Operations Support
Task Order Performance Work Statement (PWS)

1. Purpose: The objective of this task order is to provide information technology (IT) solution support services.

2. Scope: The scope of this requirement is to acquire IT support services in the following task areas:

- Task 1: Program Management
- Task 2: Requirements Support
- Task 3: Field Support
- Task 4: Operations & Data Center Support
- Task 5: Cybersecurity and Software Management Support
- Task 6: Lifecycle Management Support

3. Requirements: The contractor shall provide the following services:

3.1 Program Management: The contractor shall provide the following program management support services and ensure satisfaction of all PWS tasks, including program management.

3.1.1 Kick-Off Meeting: The contractor shall schedule, coordinate and host a Kick-Off meeting at a location approved by the Government. The meeting will provide an introduction between the contractor personnel and Government personnel. The meeting will provide the opportunity to discuss technical, management, security logistics and travel authorizations and reporting procedures. At a minimum, the attendees shall include representatives from the AFPOA Directorates, Contracting Officer, Contracting Officer Representatives, General Services Administration/Direct Client Support Representative and other relevant Government personnel.

3.1.2 Monthly Status Report (MSR): The contractor shall provide a MSR for all tasks describing all service level metrics required throughout this PWS, status of execution under the contract, any known contract issues or deficiencies, expected information or support required from the Air Force, high level funding status (where appropriate), and a risk matrix with details on medium/high risks. The contractor shall submit an individual MSR for each task to the task lead of the associated PWS task. The contractor shall distribute the MSR for work efforts assigned by the 5th business day of the month. The MSRs shall include:

- Progress since last report
- Risks that may delay the work effort's completion and proposed solutions
- Steps to accomplish each work effort, percentage complete status, and the target date for each work effort's completion

- Concerns, issues, delays, risks, and proposed resolutions of identified problems or concerns
- Project activities, Key Personnel and planned expenditures by task/subtask for the next month
- Personnel changes that impact ability to execute/perform responsibilities
- Changes to the program management plan and/or the quality control plan
- For each employee: labor category, skill level, hours worked (denoting on or off site), and cumulative hours worked
- Problem Notification Reports
- Projected cost of each Contract Line Item Number for the upcoming quarter.
- List of applications/systems/software management status and estimated completion date
- Issues affecting system accreditation and authorization and software management (include description, impact and recommended solution)
- Any changes to requirements with description of issues that impact ability to execute/perform responsibilities as outlined
- Identifying contractors trained, subject matter and date trained

3.1.3 Program Management Plan: The contractor shall submit a program management plan describing the overall methods used to meet the PWS requirements in less than three pages. This document is an evolutionary document that will be reviewed and updated throughout the lifecycle of this requirement. This will include partnering and subcontracting plans and identifying the tasks that they will be performing. A draft shall be provided with the proposal.

- ***Deliverable #1**: **Program Management Plan***

3.1.4 Schedule: The contractor shall submit a schedule for major tasks in the PWS. This shall include all specific instances in the PWS where a specific date or days are task order award are identified. A draft shall be with the proposal.

- ***Deliverable #2**: **Schedule***

3.1.5 Quality Control Plan: The contractor shall submit a quality control plan detailing how the contractor will ensure quality products and services are provided to the Government in less than five pages. A draft shall be provided after task order execution.

- ***Deliverable #3: Quality Control Plan***

3.1.6 Meetings: The contractor shall provide meeting support and shall accomplish the following:

3.1.6.1 Shall participate in status meetings, not more than once a week, to review current and planned activities for the major task areas.

3.1.6.2 Shall prepare an “Activity Report Brief” at least one business day prior to the Status Meeting that details the results and planned actions for the contractor’s team supporting the tasks. Typical topics may include status, stoplight charts, and planned acquisitions and changes/updates to the program management plan. The information in this report shall be considered the foundation for the monthly status reports.

- ***Deliverable #4: Activity Report Brief***

3.1.6.3 Shall conduct and/or attend monthly program reviews to present status of tasks.

3.1.6.4 Shall conduct and/or attend initial Assessment and Authorization (A&A) and Government requested software management task kick-off meetings and weekly meetings thereafter to present ongoing project status until each project is completed (Applicable to the A&A Task).

3.2 Requirements: The contractor shall support the following Requirements Division (DFR) tasks:

- Commanders Tool Kit (CCTK)
- Application Development

3.2.1 CCTK: The Air Expeditionary Force (AEF) Online; CCTK provides commanders with an effective way to monitor and manage their unit's deployment readiness and provides Airmen with a single-point access for requisite deployment readiness information within the Personal Deployment Preparedness Tool (PDPT) via AEF Online. The User Management System (UMS) application provides a common login experience and user management tool for all applications. The Deployment Readiness Checklist (DRC) application allows online mobility processing at the unit, along the travel path, and at the deployed location. The Online Mobility Folder (OMF) application provides the ability to electronically store and transfer numerous documents that are needed for mobility processing eliminating the need to carry these documents by hand.

3.2.2 Application Development: The contractor shall provide application developers in support of the CCTK mission. The contractor shall possess and maintain a Department of Defense (DOD) 8570 Cyber Security certification in support of the CCTK mission. The contractor shall have upon hire and maintain SECRET security clearance.

3.2.2.1 Task Lead: The Task Lead shall provide leadership and management support for contractor personnel assigned in support of the Application Development task. The Task Lead shall provide supervision and training of assigned personnel to ensure a high level of proficiency and customer service. The task lead shall ensure that the MSR is submitted each month.
3.2.2.2 Shall develop code modules in C-Sharp programming language using Microsoft Visual Studio to provide new functionality (requirements), modify, correct, and refactor defect or bug fixes for the CCTK, PDPT, UMS, DRC, and the OMF applications within AEF Online IAW software engineering practices provided by the government and according to direction provided by the government lead.

- ***Deliverable #5**: **All C-Sharp Code Modules***

3.2.2.3 Shall develop code modules in Standard Query Language (SQL) using SQL Server Management Studio to provide new functionality (requirements) and defect/bug fixes for the CCTK, PDPT, UMS, DRC, and OMF applications within AEF Online IAW software engineering practices provided by the government and according to direction provided by the government lead.

- ***Deliverable #6**: **All SQL Code Modules***

3.2.2.4 Shall analyze requirements for new functionality and defects or bugs and then provide an estimate of the Level of Effort (LOE), a delivery date that would be required, and the approximate length of time it would take to design, develop, test, and field code that implements this new functionality, or defect or bug fix in the CCTK, PDPT, UMS, DRC, and OMF applications within AEF Online.

- ***Deliverable #7**: **All Estimated LOE and Delivery Date***

3.2.2.5 Shall analyze, troubleshoot and provide technical solution for new functionality (requirements) in order to design, develop, test, and field code that implements this new functionality for the CCTK, PDPT, UMS, DRC, and OMF applications within AEF Online.

- ***Deliverable #8: All Status Reports and Analytics***

3.2.2.6 Shall analyze, troubleshoot and provide defect resolution and brief the results to the government lead for defects/bugs in order to design, develop, test, and field code that fixes the defect or bug for the CCTK, PDPT, UMS, DRC, and OMF applications within AEF Online.

- ***Deliverable #9**: **All Status Reports and Analytics***

3.2.2.7 Shall communicate and brief system requirements, system capabilities, system limitations and risks with customers and senior leadership.

- ***Deliverable #10: All Analytic materials and logs***

3.2.2.8 Shall quantify, categorize, and describe user requirements in a manner that enables the government to make an informed decision regarding the performance of new functionality.

- ***Deliverable #11**: **All presentation materials and Notes***

3.2.2.9 Shall use government approved Commercial-Off-The-Shelf (COTS) tools such as Visio and PowerPoint or all other tools for systems design and development for the CCTK, PDPT, UMS, DRC, and OMF applications within AEF Online.

- ***Deliverable #12**: **All reference material or links used***

3.2.2.10 Shall ensure all developed code receive Risk Management Framework (RMF) cybersecurity authorization. The contractor shall document their findings and provide to the government lead.

- ***Deliverable #13**: **All guides and scan results used***

3.2.2.11 Shall develop code to be device agnostic (enables the code to run on different hardware from different manufacturers) to every extent possible by not using proprietary Application

Program Interface (APIs). The contractor shall provide a list of all APIs used to the government lead.

- ***Deliverable# 14**: **All reference APIs used***

3.2.2.12 Shall develop all code necessary to perform any Extract Transform & Load (ETL) actions necessary for proper operation of the applications. The contractor shall provide all C# code and SQL modules used.

- ***Deliverable #15**: **All C# Code and SQL Modules used***

3.2.2.13 Shall create a Test Plan IAW the government provided standard to guide testing. The Test Plan shall provide the following minimum information: what to test, how to test, when to test and who will do the testing of the software requirements. The standard is IEEE829 format and additional information will be provided upon execution of the task order.

- ***Deliverable #16: All Test Plans and Steps for testing each requirement or defect/bug***

3.2.2.14 Shall attend all code releases when code is migrated to the test, development and production environment's which often occur after standard duty hours of 0730 to 1630 hrs. CST.

3.2.2.15 Shall configure data mapping details documented in the design documents.

- ***Deliverable #17**: **All Design Document Documents***

3.2.2.16 Shall review and validate government acceptance of technical requirements and design documents.

- ***Deliverable #18: All Design Document Documents***

3.2.2.17 Shall participate in and coordinate upon meeting minutes for Integrated Requirements Team (IRTs) meetings, which may be in the form of Integrated Product Team (IPT) meetings, project lead meetings, working group meetings, or other government led sessions.

3.3 Field Support Division: The purpose of this task is to provide Tier 1 troubleshooting for incoming calls and email on a continuous basis and provide support for event and change management on the AFPOA production environment. The list of applications supported is provided in Appendix A3-AFPOA Application List. All contractor personnel in support of the field support task shall have upon hire and maintain a SECRET security clearance with the exception of the Business Objects task. The contractor shall support the following field support tasks:

- Task Lead
- Account Management
- A1 Service Desk Support (A1SD)
- Dash Board Operations
- Information/Knowledge Management
- Business Objects
- Access Database Support

3.3.1 Task Lead: The Task Lead shall provide leadership and management support for contractor personnel assigned in support of the Field Support task. The Task Lead shall provide supervision and training of assigned personnel to ensure a high level of proficiency and customer service. The Task Lead shall possess the Information Assurance (IA) Technical Level II certification IAW the Workforce Improvement Program (http://www.dtic.mil/whs/directives) and AFMAN 17-1303, Cybersecurity Workforce Improvement Program, May 2016 (http://www.e-publishing.af.mil). The task leader shall ensure that the MSR is submitted each month.

3.3.1.1 Shall utilize existing task instructions and procedural guidelines for use in instructing newly assigned personnel and administers recurring training for contractors performing Service Desk Support.

3.3.1.2 Shall ensure existing Tactics, Techniques and Procedures (TTPs) are accurate and updated as changes in processes occur. Changes and updates will be provided by and/or coordinated with the Government.

3.3.1.3 Shall ensure contractors are logged in to the telephone system and available to take incoming calls 24x7x361 (362 days during leap years).

3.3.1.4 Shall ensure the average "Not Ready" state is ≤ 22% on a daily basis for each contractor.

3.3.1.5 Shall ensure each contractor does not exceed five (5) "Ring on No Answer" (RONA) calls during all shifts, 7 days per week.

3.3.1.6 Shall ensure customers do not experience long wait times (considered to be > 3 minutes) in the phone queue.

3.3.1.7 Shall maintain an incoming call queue count of ≤ 8 callers for any 30 minute interval during the Contiguous United States (CONUS) shift.

3.3.1.8 Shall ensure contractors are available to provide Common Access Card (CAC) support (CAC unlocks/resets) within 3 minutes of customer arrival in the A1SD during the CONUS shift, Monday through Friday.

3.3.1.9 Shall notify the Dashboard Operator and all contractors performing service desk support when customers report an unscheduled incident impacting system availability and/or accessibility. In addition, the Task Lead shall ensure contractors are notified when the incident is resolved.

3.3.1.10 Shall ensure a TTP or knowledge article is created and coordinated with the Government within 5 business days when new systems/applications are assigned to the A1SD.

- ***Deliverable #20: TTP and/or Knowledge Article***

3.3.1.11 Shall provide quality control reports identifying open tickets, incidents over 30 days old, tickets not assigned and requests over 30 days old on Wednesday's each week.

- ***Deliverable #21: Quality Control Reports for Trouble Tickets***

3.3.1.12 Shall provide trouble ticket report identifying category of tickets created and total tickets submitted no later than the 1st Thursday of each month.

- ***Deliverable #22**: **Trouble Ticket Report for Leadership Meeting***

3.3.2 Account Management: Contractor supporting the account management task shall possess the IA Technical Level II certification in IAW the Workforce Improvement Program (http://www.dtic.mil/whs/directives) and AFMAN 17-1303, Cybersecurity Workforce Improvement Program, May 2016 (http://www.e-publishing.af.mil).

3.3.2.1 Shall provide customers with assistance to obtain a user account required to access the Air Force Network (AFNET) in accordance with existing TTPs.

3.3.2.2 Shall provide the customer with the policies, forms and guidance required for new application account requests.

3.3.2.3 Shall review all documents submitted for access to human resource applications, ensuring information assurance certification and appropriate signatures have been obtained on required documents. The forms shall be submitted to the appropriate point of contact for processing and then stored in the account management database.

3.3.2.4 Shall apply established security groups to specific shared files with the appropriate permissions in shared files and the global address listing.

3.3.2.5 Shall ensure accounts are created accurately and troubleshoot access and connectivity issues to the Air Force network and/or supported applications.

3.3.2.6 Shall implement IT security policies and procedures to ensure protection of information transmitted to the installation, among organizations on the installation, and from the installation using Local Area Networks (LAN), Wide Area Networks (WAN), the World Wide Web, or other communications modes.

3.3.2.7 Shall limit privileged access to systems/applications (i.e., operating system, system parameter and configuration files, and databases), utilities, and security-relevant programs/data files to authorized personnel and will maintain required supporting documents for each account created in the account management database on the restricted drive.

3.3.3 Service Desk Support. The contractor shall provide service desk support for all three shifts: Contiguous United States (CONUS), Pacific Air Forces (PACAF) and United States Air Forces in Europe (USAFE). The contractor:

3.3.3.1 Shall answer incoming calls and respond to email incidents and requests for assistance in accessing or utilizing applications supporting the military and civilian human resource applications.

3.3.3.2 Shall create a trouble ticket in the incident management application for each phone call and email incident, problem, or request reported by the customer. Trouble tickets shall be categorized and assigned in accordance with established TTPs.

- ***Deliverable #23**: **Trouble Tickets***

3.3.3.3 Shall create, reset and unlock user accounts and passwords for applications assigned.

3.3.3.4 Shall triage customer concerns and if the problem is determined not to be related to a technical issue with AFPOA managed applications, the caller shall be redirected to the appropriate point of contact. The contractor shall include information and advice on how to communicate the problem to ensure the caller and the point of contact understands the problem.

3.3.3.5 Shall monitor the A1SD group email inbox daily and create trouble tickets for all incidents, requests and problems submitted and resolve or escalate trouble tickets to Tier II technical personnel.

3.3.4 Data Base Owner (DBO) Shift Support: The contractor shall provide 24x7 dashboard operations support services during each of the three shifts: CONUS, PACAF and USAFE.

3.3.4.1 CONUS Shift DBO Support: The CONUS Shift DBO shall perform dashboard operations, event and change management support services. Event management occurs when the availability and/or accessibility of an AFPOA supported system or application is negatively impacted. Change management involves scheduling maintenance, patching and upgrades of systems and applications on the APFOA production environment.

3.3.4.1.1 Shall review, modify and store the DBO TTP on the restricted drive. The TTP shall be updated annually, or as processes change.

3.3.4.1.2 Shall facilitate processing of events, to include opening the event in the A1SD Dashboard, tracking and updating the event as status changes.

3.3.4.1.3 When required the CONUS shift DBO shall send the Notice to Airman (NOTAM) within 15 minutes of notification.

3.3.4.1.4 Shall ensure event information is reviewed and updated daily for accuracy. Incidents are reported or identified to the DBO via customer phone calls, email, and/or by AFPOA technical personnel.

3.3.4.1.5 Shall transfer event information from the A1SD Dashboard to the Unscheduled Interruption Log (located on the restricted drive) when the event is closed.

3.3.4.1.6 Shall review and monitor the A1SD Dashboard to ensure current and accurate data (on-call listing, critical server listing, functional system administrator listing, guidance, etc.) is entered no later than the second Monday of each month.

3.3.4.1.7 Shall ensure the PACAF and USAFE DBOs have the necessary information and guidance to manage incidents impacting application availability and/or accessibility prior to the PACAF shift change Monday through Friday.   All incidents shall be updated on the A1SD Dashboard and information and resource materials provided and briefed during shift change.

3.3.4.1.8 Shall update and provide the correct/updated information when the PACAF or USAFE shift DBO identifies information that is inaccurate or confusing on the A1SD Dashboard.

3.3.4.1.9 Shall update, review and post the daily System Status Report to SharePoint.

- ***Deliverable #24: System Status Report***

3.3.4.1.10 Shall prepare and deliver reports and metrics related to event management (metrics/trends) to include system availability, accessibility and unscheduled interruptions each month. The reports are saved on a shared drive for the monthly leadership meeting and are due on the 1st Thursday of each month.

- ***Deliverable #25: Event Management for Leadership Meeting***

3.3.4.1.11 Shall provide Authorized Service Interruption (ASI) assistance to Maintenance Control (MC) as needed (normally 3-5 days each month) when processing and coordinating ASIs.

3.3.4.1.12 Shall submit and track network change requests. This involves working to create positive relationships with AFNET and AFPOA mission partners to help facilitate discussions regarding network change requests with mission partners and other personnel.

3.3.4.1.13 Shall coordinate, submit, and modify network change requests and store information in the change sponsor Access database on the shared drive.

3.3.4.1.14 Shall provide assistance in MC. The contractor shall review the AFPOA MC Plan (provided by the Government). The MC plan identifies the AFPOA processes and procedures to maintain control in the identification, coordination and scheduling of all maintenance actions and is located on the shared drive.

3.3.4.1.15 Shall assist with scheduling, processing, and coordinating authorized service interruptions. Review incoming ASIs for administrative and technical compliance and verify ASIs contain required information.

3.3.4.1.16 Shall assist the Government in updating the ASI database to include users, assets, sub-systems and organization information.

3.3.4.1.17 Shall assist the Government in preparation for the weekly Change Advisory Board (CAB). Upon completion of the CAB, the Contractor shall assist the Government in approving and scheduling ASIs for action.

3.3.4.2 PACAF & USAFE Shift DBO Support: The contractor shall provide DBO support services to the PACAF (1400-2300) and USAFE (2230-0730) shifts. Additionally, PACAF and USAFE shifts shall provide event management support consisting of monitoring performance tools (currently using Hewlett-Packards Open View Manager) in addition to A1SD support.

3.3.4.2.1 The PACAF and USAFE shift DBOs shall ensure a shift change is conducted 15 minutes prior to their shifts ending. The briefing shall include updates related to open incidents, changes in procedures, and/or questions that arise throughout their shift.

- ***Deliverable #26: Shift Briefings***

3.3.4.2.2 Shall ensure information related to event management is input to the DBO Bulletin Board. (The DBO Bulletin Board is an Excel spreadsheet on the shared drive that is used for situation awareness between DBOs and AFPOA technical personnel).

3.3.4.2.3 Shall perform A1SD support services for incoming calls and email when not actively working events.

3.3.4.2.4 Shall monitor the MC group inbox continuously throughout their shift to ensure responses are provided for messages identifying critical outages or events that may impact system/application availability and/or accessibility.

3.3.4.2.5 Shall review the A1SD Dashboard information, guidance, listings, etc., and if information is missing or is confusing, notify the CONUS shift DBO.

3.3.4.2.6 Shall update and/or open events on the A1SD Dashboard per TTP and A1SD Dashboard instructions.

3.3.4.2.7 Shall monitor and respond to messages on system monitoring tools (currently using Hewlett-Packard's Open View Manager). The contractor shall ensure they are adhering to instructions in the A1SD Database and TTP.

3.3.4.2.8 When A1SD Dashboard instructions indicate a NOTAM is required, the contractor shall send the NOTAM within 30 minutes of identifying an event.

3.3.4.2.9 Shall update and post the System Status Report to SharePoint when and event is opened and/or when requested by the Government.

3.3.4.2.10 Shall notify the CONUS shift DBO upon identification of outdated information in the A1SD Dashboard, or if there are questions related to processing Events, MC email, or TTP guidance.

3.3.5 Information &Knowledge Management Support: The contractor performing this responsibility shall be proficient with applications used for these duties, which include, but are not limited to, Microsoft Active Directory, Microsoft Office (Front Page, Access, Excel, PowerPoint, SharePoint, Visio and Word).

3.3.5.1 Shall open new databases, and create services through which content can be creatively combined, searched and correlated as directed.

3.3.5.2 Shall ensure ad hoc reports and metrics requested are provided are in an easy to read format and per established TTP guidelines. Reports shall be submitted to requestor within 5 business days of request.

- ***Deliverable #27**: **Ad Hoc Reports***

3.3.5.3 Shall extract data from the incident management application, the VoIP system, or other A1SD databases and store them on the restricted drive for reporting and metrics purposes.

3.3.5.4 Shall make modifications to the A1SD Dashboard configuration within 10 business days when new requirements are identified by the Government.

3.3.5.5 Shall verify and validate and document configuration changes for each Access database as modifications are made and shall review and verify information accuracy annually (in December). The contractor shall avoid duplication of data.

3.3.5.6 Shall maintain the A1SD SharePoint page and review/update on a monthly basis, to include the Frequently Asked Questions (FAQs), self-service information, and documents supporting the A1SD and mission partners.

3.3.5.7 Shall maintain a knowledge database on the shared drive for user guidance and that provides customers and A1SD support personnel with self-help solutions and assistance in resolving non-complex problems. Information will provided by the Government.

3.3.5.8 Shall review and validate the knowledge articles six months after creation and every six months thereafter.

3.3.5.9 Shall be responsible for maintaining backups of all databases, metrics and process documents and making them accessible to the Government. A report identifying the databases and back-up dates shall be submitted to the Branch Chief on the last Friday of each month.

- ***Deliverable #28: Database Backup Report***

3.3.6 Database Operations (DBO) Support: Contractor personnel supporting database operations shall require enhanced/administrative privileges as designated under DOD 8570.01-M as IAT-Level II which will require to maintain 8570 certification. Database System Administrators may be required to provide 24 hours a day, 7 days per week, and 365 days per year on-site support with on-call support during evenings and on holidays. Weekend and shift work may be required on a rotational basis. The contractor:

3.3.6.1 Task Leader: The Task Lead shall provide leadership and management support for contractor personnel assigned in support of the DBO support tasks. The Task Lead shall provide supervision and training of assigned personnel to ensure a high level of proficiency and customer service. The task leader shall ensure that the MSR is submitted each month.

3.3.6.2 Shall provide technical and database system administration support for all AFPOA/AFPC Network Enterprise systems.

3.3.6.3 Shall support, maintain, and enhance the software environment supporting the AFPOA/AFPC Network Enterprise. The scope of this task includes: managing application software installations, configuration, and upgrades; establishing software test environments; and integrating software problem reporting procedures, plans and tools installation/integration. Research, analyze, test, document system issues and keep TTPs current.

3.3.6.4 Shall use various tools to monitor database instances and all other areas requiring database system administration oversight. Tasks to be performed consist of monitoring and ensuring that databases, associated storage systems, and peripheral equipment are operational as required; databases are backed up and restored as necessary and planning for future enhancements and upgrades to the existing systems.

3.3.6.5 Shall provide support to the Information Technology Disaster Recovery (ITDR) yearly exercise. System administration and location for the ITDR exercise will require unclassified and support.

3.3.6.6 Shall perform general IT Support and Database Administration (DBA) maintenance functions as required, including database performance tuning and trouble analysis and resolution to support key Air Force/A1, Personnel, Services, and Manpower applications, and to support the Air Force database tables that are used within Business Objects, and assistance with the maintenance of unique databases such as Trouble ticket application, and conversion of database applications into Oracle when needed.

3.3.6.7 Shall provide analysis and database administration support for deployment and sustainment of the Business Objects (BO) repositories and universes. The major work requirement will involve database additions and modifications as required to pull data from Human Resources (e.g. Defense Civilian Personnel Data System and Customer Service Unit) and other sources (e.g., USA Staffing, Manpower Programming and Execution System (MPES), etc.) to meet the needs of the Air Force.

3.3.6.8 Shall provide technical expertise to support the development of architecture and deployment plans best suited for BO applications.

3.3.6.9 Shall provide technical expertise to support the development of a strategy for maintaining and synchronizing the various Business Objects repositories and universes.

3.3.6.10 Shall provide technical expertise to support the development of a strategy for deploying BO throughout the Air Force civilian personnel community (internal and external users). The Contractor shall assist in the development of a strategy for implementing security within BO universes for both internal and external, personnel and non-personnel communities. The Contractor shall provide advice on maintaining and fine-tuning these strategies.

3.3.6.11 Shall provide technical expertise to support with the design of the BO universes by accomplishing DBA tasks such as creating stored functions and stored procedures to optimize BO performance.

3.3.6.12 Shall maintain change control on all database baseline scripts associated with the BO repositories and any additional Air Force unique Oracle database tables established to support the query and reporting needs of the Air Force. The Contractor shall install databases in various environments (e.g., development, test, acceptance, production, and training) as needed, and follow change control plan across environments.

3.3.6.13 Shall monitor and maintain database interfaces to HR databases to support the Air Force unique systems or databases.

3.3.6.14 Shall document any data schema changes (specific system configuration changes) that may affect either the Air Force unique civilian personnel systems or the BO repositories or universes. Documentation should contain identification of refresh data extraction changes from the appropriate source (e.g., DCPDS, USA Staffing, MPES, etc.) to include table/view and column/attribute references highlighting any changes resulting from patches or releases.

3.3.6.15 Shall plan and support the standup of the BO repositories and universes and other AF unique applications at a designated Disaster Recovery Site during practice or real- life events.

3.3.6.16 Shall provide expert technical analysis, options, guidance and support for projects such as data center consolidation, cloud initiative, application re-homing, and decommissioning of applications.

3.3.6.17 Shall provide technical services for the BO XI3/BI4 environment; troubleshoot and evaluate BO XI3/BI4 system and reporting performance issues.

3.3.6.18 Shall assess infrastructure to include platform impact, network impact, security authentication, access assignment mapping, and server sizing and performance as it pertains to the Performance Management environment.

3.3.6.19 Shall provide assistance with installation and configuration of BO BI4 in a Linux virtual environment, to include the single-sign-on solution and configuration for BO BI4.

3.3.7 Business Objects Support: The contractor**:**

3.3.7.1 Shall conduct User Interface (UI) assessment as necessary.

3.3.7.2 Shall troubleshoot and evaluate BO (either BO versions XI3, BI4 or both) system performance issues if the BO Technical Support office is unable to evaluate and access infrastructure.

3.3.7.3 Shall assess infrastructure to include platform impact, network impact, security Public Key Infrastructure (PKI) authentication, access assignment mapping, and server sizing and performance as it pertains to BO, either XI3, BI4 or both to include Apache Tomcat configuration.

3.3.7.4 Shall assist with installation and configuration of BO BI4 development, test and production systems in a Linux virtual environment.

3.3.7.5 Shall assist in the conversion of metric and advance formatted existing BO Corporate Document Library reports from BO XI3 to BI4.

3.3.7.6 Shall assist with the BO BI4 design and maintenance of universe and univex.

3.3.7.7 Shall provide a written assessment on all work performed during the entire consultant visit. Due within 10 business days after consulting visit is completed. Assessment will be provided 100% of the time.

- ***Deliverable #29: Assessment***

3.3.8 Access Database Support

One contractor shall be assigned to provide Access database support. The contractor shall have high proficiency with applications used for these duties, which include, but are not limited to, Microsoft Active Directory, Microsoft Office (Front Page, Access, Excel, PowerPoint, SharePoint and Visio).

3.3.8.1 Shall ensure at hoc reports and metrics requested are provided are in an easy to read format and per established guidelines.

3.3.8.2 Shall extract data from the incident management application, the VoIP system, or other databases.

3.3.8.3 Shall document and validate the configuration of each Access database annually and updated on a routine basis as modifications are made.

3.3.8.4 Shall update the A1SD Dashboard configuration as new requirements are identified by the Government.

3.3.8.5 Shall update and maintain the A1SD SharePoint page; to. Include the FAQs, self-service information, and documents supporting the A1SD and mission partners.

3.3.8.6 Shall ensure documents provided and stored on A1SD SharePoint shall be reviewed and updated every six months, or as changes are made to ensure information is accurate and up to date.

3.3.8.6 Shall ensure no more than three documents are out of date or incorrect in a six month period.

3.3.8.7 Shall develop and maintain TTPs related to duties assigned. TTPs shall be reviewed and updated annually, or as processes change to ensure information is accurate and up to date.

3.3.8.8 Shall maintain a knowledge database for user guidance, information and documentation that provides customers and Service Desk personnel with self-help solutions and assistance in resolving non-complex problems identified by the technical support personnel or customer.

3.3.8.9 Knowledge articles shall be reviewed and validated 6 months after creation and every 6 months thereafter.

3.3.8.10 Shall avoid duplication of data. This requires a review and update of data on a recurring basis, opening of new databases, and create services through which content can be creatively combined, searched and correlated.

3.3.8.11Shall be responsible for maintaining backups of all databases, metrics and process documents and making them accessible to the Government.

3.4 Operations Support & Data Center Operations: The contractor shall provide support for the following Operations & Data Center Operations tasks:

- Task Lead
- Windows Operations
- Systems Operations

3.4.1 Task Leader: The Task Lead shall provide leadership and management support for contractor personnel assigned in support of the Operations Support & Data Center Operations support tasks. The Task Lead shall provide supervision and training of assigned personnel to ensure a high level of proficiency and customer service. The task leader shall ensure that the MSR is submitted each month.

3.4.2 Windows Operation: The objective of this task is to support, maintain, and enhance the Microsoft Windows-based Server Operating Systems and associated hardware environment supporting the AFPOA Network Enterprise. The scope of this task includes the following but is not limited to: managing Microsoft Windows-based Server Operating System installations, configuration, and upgrades; establishing Microsoft Windows-based operating system test environments; and integrating operating system and hardware problem reporting procedures, plans and tools installation/integration. Research, analyze, test, document system issues and keep Technical, Tactics, and Procedures (TTPs) current.

All contractor personnel supporting the Windows Operations task shall possess a U.S. security clearance at the minimum level of "Secret." Contractor personnel will require administrative privileges as designated under DOD 8570.01-M as Information Assurance Technical (IAT)-Level II, and are required to maintain 8570 certification. A Bachelor's Degree from an accredited institute in an area applicable to this position (e.g. information systems, computer science, math, or engineering) is preferred but cannot be used a substitute for the requirements in paragraphs 3.4.2.2, 3.4.2.3, and 3.4.2.4.

Tasks to be performed apply to all AFPOA Enterprise Windows and ESX-based systems being supported by the Windows Operations Branch. Normal duty hours are 0700hrs – 1600hrs Central Standard Time (CST), Monday through Friday. System administrators may be required to provide 24 hours a day, 7 days per week, and 365 days per year on-site support with on-call support during evenings and on holidays. Weekend and shift work may be required on a rotational basis.

3.4.2.1 The contractor shall provide senior level system administration support for all AFPOA enterprise Windows and ESX-based systems. The scope of this task consists of monitoring and ensuring that servers, associated storage systems, and peripheral equipment are operational as required, systems are backed up and restored as necessary, hardware is configured in an optimal manner, planning for future enhancements and upgrades to the existing systems, configuring new hardware once received, and other tasks as required by AFPOA.

3.4.2.2 Shall have Microsoft System Engineer (MCSE) or System Administrator (MCSA) certifications.

3.4.2.3 Shall have the VMware Certified Professional (VCP) 6 or higher certification. S

3.4.2.4 Shall have experience with Microsoft Active Directory, Microsoft Internet Information Systems (IIS 7, 8, and 8.5)

3.4.2.2 Windows-Based Server Environment Support: The Windows-based server environment consists of over 550 full form servers, blade servers (including virtual server hosts), and VMware vSphere virtual servers as well as over 300 VMware vSphere Virtual Desktop Infrastructure (VDI) virtual desktops. Some servers utilize Microsoft file and database clustering services. Tools and utilities to perform administration duties on all server types include, but are not limited to: Microsoft Active Directory Administration tools and utilities (including Microsoft Management Console (MMC)), Shavlik Netchk, ERDisk, Hewlett-Packard (HP) OpenView, Trouble Ticket application tools, HP Systems Insight Management, Veritas Storage Foundations, VMware vSphere, VMware vCenter Operations Management Suite, VMware Horizon Suite, VMware ESX/ESXi, SureSync, ARKIIS, McAfee Anti-Virus, and various server imaging software. All administration software and tools shall be provided. The contractor:

3.4.2.2.1 Shall provide technical and system administration support for Web applications using Microsoft Internet Information Systems (IIS) and Apache Tomcat for all AFPOA Network Enterprise systems in a tiered, multi-system, multi-web engine environment.

3.4.2.2.2 Shall provide Active Server Pages (ASP), Microsoft .NET Framework, Visual Studio (VS), C++, C Sharp, Java Server Pages (JSP), and Hypertext Markup Language (HTML) web application support to include configuration, maintenance, and troubleshooting through interaction and/or use of available tools.

3.4.2.2.3 Shall manage PKI certificates for new and existing operating system and web applications. Shall maintain and implement data sources, API integration, and extensions.

3.4.2.2.4 Shall maintain and troubleshoot the operation and performance of web applications and associated web application resources through IIS Manager and available tools.

3.4.2.2.5 Shall update, annotate, track and modify all trouble ticket application tickets submitted for Windows Operations Support.

3.4.2.2.6 Shall provide Windows administration support to include installation, support, and maintenance of Windows-based operating systems.

3.4.2.2.7 Shall maintain and enhance the computer hardware and Windows-based operating system environments for legacy and modern systems.

3.4.2.2.8 Shall provide configuration control, sustainment, performance and tuning on system peripherals and subsystems.

3.4.2.2.9 Shall maintain Windows-based operating system configuration using system tools, utilities and operating system commands.

3.4.2.2.10 Shall manage and coordinate hardware, software and application changes.

3.4.2.2.11 Shall perform and document configuration management changes on the application and software installations and plan and respond to service outages

- ***Deliverable #29: Configuration Management Change Report***

3.4.2.2.12 Shall diagnose Windows-based software and hardware failures to resolution.

- ***Deliverable #30: Software & Hardware Failures Resolution Report***

3.4.2.2.13 Shall use or assist in creating local documentation to establish Tactics, Techniques, and Procedures (TTPs) used to support, maintain, and enhance the Microsoft Windows-based Server Operating Systems and associated hardware environment supporting the AFPOA Network Enterprise.

3.4.2.2.14 Shall assist in the creation, installation and un-installation of applications, software releases and patches using sound Configuration Management practices.

3.4.2.2.15 Shall research, analyze, develop, test, and implement data integration system to system level in support of current or future AFPOA requirements to support continuous process improvement. The contractor shall provide results to the technical lead.

- ***Deliverable #31: Results Report***

3.4.2.2.16 Shall provide user account and group management for systems. This includes add/disable/delete user and group accounts, passwords, change permissions and access control.

3.4.2.2.17 Shall provide performance management support. This task includes using system diagnostics tools and reporting hardware or software problems with the appropriate vendor for support. The contractor shall enhance the system performance, when applicable.

3.4.2.2.18 Shall support Windows file system management. This task includes modifying permissions on directories and files and creating and modifying file systems.

3.4.2.2.19 Shall provide Windows system security administration.

3.4.2.2.20 Shall maintain the system security by monitoring server access and reviewing necessary logs.

3.4.2.2.21 Shall implement and ensure security preventive measures are fully functioning.

3.4.2.2.22 Shall ensure all Windows servers in AFPOA maintain adequate security status and compliance IAW Air Force Manual 17-1301, Air Force Network Operating Instructions, AFNOSC TCNO/CTO/NTO/IAVM, and AFPOA direction. This task includes the installation of vendor operating system patches and firmware updates.

3.4.2.2.23 Shall mitigate vulnerabilities/security findings identified on Assured Compliance Assessment Solution (ACAS) Nessus scans, Defense Information Systems Agency (DISA) Security Technical Implementation Guide (STIG), and Security Content Automation Protocol (SCAP) Compliance Checker in preparation for Risk Management Framework (RMF) Authorization to Operate (ATO) package submissions.

3.4.2.2.24 Shall provide system support for scheduled functional system tests (FST).

3.4.2.2.25 Shall provide assistance to users of legacy and Windows systems.

3.4.2.2.26 Shall provide application system administration support required to perform System Administration functions.

3.4.2.2.27 Shall provide system design on hardware installation and configuration on servers.

3.4.2.2.28 Shall perform Windows disk management. This task includes disk mirroring and configuring internal and external disk storage with redundant access paths.

3.4.2.2.29 Shall create, modify and maintain scripting to automate Windows System Administration tasks and functions.

3.4.2.3 System Operations: All contractor personnel supporting the System Operations task shall obtain a U.S. security clearance at the minimum level of "Secret." Contractor personnel supporting paragraphs: 3.4.2.3.1, 3.4.2.3.2, 3.4.2.3.3, and 3.4.2.3.5, will require administrative privileges as designated under DOD 8570.01-M as Information Assurance Technical (IAT)-Level II, and are required to maintain 8570 certification. Contractor personnel supporting System Operations task paragraph 3.4.2.3.4 will not require administrative privileges as designated under DoD 8570.01-M, and are not required to maintain 8570 certification. The contractor shall provide a single contractor representative to act as a task leader for the System Operations task. The contractor shall perform the following system operations support services:

3.4.2.3.1 UNIX Administration support: The contractor shall provide senior level UNIX Administration support during normal duty hours, 0730-1630 Central Standard Time (CST), Monday through Friday. In addition, the contractor shall provide minimal shift work coverage from 0700-1500 CST on weekends and holidays. The contractor will provide on-call support after duty hours to include evenings, weekends and on holidays. The contractor:

3.4.2.3.1.1 Shall provide UNIX Administration support to include installation, support, and maintenance of approximately 200 Linux, HP-UX, Solaris, and UNIX-based operating systems.

3.4.2.3.1.2 Shall maintain and enhance the computer hardware and UNIX-based operating system environments for legacy and modern systems as required.

3.4.2.3.1.3 Shall provide configuration control, sustainment, performance and tuning on system peripherals and subsystems. Maintain UNIX-based operating system configuration using system tools, utilities and operating system commands as required.

3.4.2.3.1.4 Shall perform configuration management activities to include any UNIX server hardware, software, and application changes.

3.4.2.3.1.5 Shall diagnose UNIX-based software and hardware failures to resolution. The Contractor shall use or assist in creating local documentation to establish procedures, and develop solutions to problems with UNIX-based systems.

3.4.2.3.1.6 Shall assist the application Functional System Administrator (FSA) as necessary in the installation/un-installation of applications, software releases and patches.

3.4.2.3.1.7 Shall provide user account and group management as required for systems. This management includes add/disable/delete user and group accounts, passwords, change permissions and access control.

3.4.2.3.1.8 Shall perform performance management as required. This management includes using system diagnostics tools and reporting hardware or software problems with appropriate vendor for support. The contractor shall use the Hewlett-Packard Operations Manager (HPOM) software suite and/or other tools that may be available or become available for use to monitor and identify servers that are experiencing problems during shift. The contractor shall enhance system performance when applicable.

3.4.2.3.1.9 Shall support UNIX file system management. This management includes modifying permissions on directories and files, and creating and modifying file systems.

3.4.2.3.1.10 Shall provide UNIX system security administration as required. Maintain system security by monitoring server access and reviewing necessary logs. The contractor shall implement and ensure security preventive measures are fully functioning. Ensure all UNIX servers maintain adequate security status and compliance IAW AIR FORCE MANUAL 17-1301, Cyberspace COMPUTER SECURITY (COMPUSEC), Air Force Network Operating Instructions, AFNOSC cyber orders to include TCNO/CTO/NTO/IAVMs, and AFPOA direction. Actions include installation of vendor operating system patches and firmware updates. The contractor shall apply 95% of applicable TCNOs, IAVMs and security hotfixes successfully by mandated compliance date.

3.4.2.3.1.11 Shall provide RMF UNIX system administration support on ATO packages.

3.4.2.3.1.12 Shall provide system support for scheduled functional system tests (FST).

3.4.2.3.1.13 Shall provide assistance to users of legacy and UNIX systems as required.

3.4.2.3.1.14 Shall provide application system administration support required to perform System Administration functions.

3.4.2.3.1.16 Shall provide system design on hardware installation and configuration on servers when required.

3.4.2.3.1.17 Shall perform UNIX disk management. This management includes disk mirroring and configuring internal and external disk storage with redundant access paths.

3.4.2.3.1.18 Shall provide and review technical solutions when necessary. Analyzes requirements and assists in preparing implementation plans as required.

3.4.2.3.1.19 Shall create, modify and maintain shell scripting to automate UNIX/Linux System Administration tasks and functions.

3.4.2.3.1.20 Shall manage UNIX system print servers.

3.4.2.3.1.21 Shall on a routine basis update, annotate, track and modify all application support tickets submitted for UNIX System Administration support as documented in the A1SD Ticket Priority Matrix. The contractor shall ensure 95% of tickets are accurately updated and annotated as required until the ticket is remedied and closed.

3.4.2.3.2 Storage Area Network (SAN) Administration support: The contractor personnel shall provide master level support during normal duty hours, 0730-1630 CST, Monday through Friday. The contractor will provide on-call support after duty hours to include evenings, weekends and on holidays. The contractor shall perform the following SAN Administration support services:

3.4.2.3.2.1 Shall install, manage, and maintain the onsite AFPOA Data Center SAN and the offsite Information Technology Disaster Recovery (ITDR) SAN consisting of 14 storage arrays (approximately 900 Terabytes of data) and associated data storage devices. The contractor shall assist systems administrators and mission partners with AFPOA SAN issues.

3.4.2.3.2.2 Shall maintain and enhance the SAN environment for legacy and modern systems as required to accomplish all associated tasks to ensure its maximum operational uptime.

3.4.2.3.2.3 Shall install, support, maintain, manage, configure storage devices and associated firmware for optimum performance and grant storage access to servers as required.

3.4.2.3.2.4 Shall work in conjunction with the backup shop on configuration and maintenance of the Virtual Tape Library (VTL).

3.4.2.3.2.5 Shall install, support, configure, manage and maintain Fiber Channel switching and routing infrastructure supporting all SAN storage devices.

3.4.2.3.2.6 Shall install, manage and maintain the necessary device and software service packs, patches, firmware and hot fixes to ensure maximum enterprise storage platform stability. The contractor shall diagnose SAN software and hardware failures to resolution.

3.4.2.3.2.7 Shall implement and ensure security preventive measures are fully functioning. Ensure all SAN devices maintain adequate security status and compliance IAW AIR FORCE MANUAL 17-1301, Cyberspace COMPUTER SECURITY (COMPUSEC), Air Force Network Operating Instructions, AFNOSC cyber orders to include TCNO/CTO/NTO/IAVMs, and AFPOA direction. The contractor shall apply 95% of applicable TCNOs, IAVMs and security hotfixes successfully by mandated compliance date.

3.4.2.3.2.8 Shall provide Risk Management Framework (RMF) SAN administration support on ATO packages.

3.4.2.3.2.9 Shall manage and use SAN management tools; including but not limited to: Nimble Storage InfoSight web interface console, Brocade Fabric Manager, HP Storage Essentials, HP

Command View, HP Storage Works (HP LeftHand), OnTap/OnCommand (NetApp), and Unisphere/Data Domain System Manager (EMC).

3.4.2.3.2.10 Shall coordinate the installation/placement of devices on the SAN with AFPOA Infrastructure Network Administrators.

3.4.2.3.2.11 Shall coordinate all storage device/software repairs with vendor.

3.4.2.3.2.12 Shall assist in preparing management briefings on current problems experienced with any storage issues. The contractor shall plan and respond to any SAN service outages.

3.4.2.3.2.13 Shall provide configuration control, sustainment, and tuning for on-line, near-line, off-line and off-site storage subsystems and resident data.

3.4.2.3.2.14 Shall evaluate and advise on storage technology advancements.

3.4.2.3.2.15 Shall provide and review technical solutions when necessary concerning storage systems.

3.4.2.3.2.16 Shall implement and ensure SAN security preventive measures are fully functioning.

3.4.2.3.2.17 Shall use the HPOM software suite and/or other tools that may be available or become available for use to monitor and identify servers that are experiencing problems during shift.

3.4.2.3.2.18 Shall on a routine basis update, annotate, track and modify all trouble ticket application support tickets submitted for SAN System Administration support as documented in the A1SD Ticket Priority Matrix. The contractor shall ensure 95% of tickets are accurately updated and annotated as required until the ticket is remedied and closed.

3.4.2.3.3 Hewlett-Packard Operations Manager (HPOM) Administration support: The contractor personnel shall provide senior level support during normal duty hours, 0730-1630 CST, Monday through Friday. The contractor will provide on-call support after duty hours to include evenings, weekends and on holidays. The contractor shall perform the following HPOM Administration support services:

3.4.2.3.3.1 Shall provide HPOM software suite administration support for a variety of data systems consisting of approximately 327 nodes located in the Data Center. HPOM software suite includes OM, OVIS, SNVP, and Reporter. The HPOM software monitors UNIX, Linux-based and Windows operating systems. In addition, HPOM monitors databases, file systems, network, and the SAN. The HPOM Administrator shall provide training on the use of the client software.

3.4.2.3.3.2 Shall manage HPOM application software installation, configuration, upgrades, patching, to include hardware needs required by all HPOM application management servers.

3.4.2.3.3.3 Shall coordinate with Functional System Administrators (FSAs), Windows Administrators, Web Administrators, Backups and Recovery Administrators, Network Administrators and SAN Administrators to ensure their monitoring and messaging requirements are met.

3.4.2.3.3.4 Shall perform template administration and configuration. This entails establishing auto actions, creating/modifying instructions and validation of messaging.

3.4.2.3.3.5 Shall ensure administrators and customers have the required training, user accounts, permissions and profiles.

3.4.2.3.3.6 Shall ensure proper functioning of the Windows and UNIX operating systems, perform shell scripting and maintain necessary scripts.

3.4.2.3.3.7 Shall troubleshoot problems and issues on HPOM monitored nodes using remote system access tools.

3.4.2.3.3.8 Shall ensure proper functioning of both Java and Motif Graphical User Interfaces (GUI's) and use both tools for administrating HPOM on monitored nodes.

3.4.2.3.3.9 Shall on a routine basis update, annotate, track and modify all trouble ticket application support tickets submitted for HPOM System Administration support as documented in the A1SD Ticket Priority Matrix. The contractor shall ensure 95% of tickets are accurately updated and annotated as required until the ticket is remedied and closed.

3.4.2.3.4 Data Center Operations Maintenance support: The contractor personnel shall provide Journeyman level support during normal duty hours, 0730-1630 CST, Monday through Friday. The contractor will provide on-call support after duty hours to include evenings, weekends and on holidays. The contractor:

3.4.2.3.4.1 Shall provide AFPOA Data Center Operational Maintenance Support to include maintaining the Heating, Ventilation, and Air Conditioning (HVAC) system; the maintain and ordering of correct Data Center power for Information Technology (IT) Hardware; maintaining Data Center physical access security system; and maintaining the master Data Center floor plan and general floor configuration. The AFPOA Data Center is approximately 11,459 square feet.

3.4.2.3.4.2 Shall provide oversight of the AFPOA Data Center operational maintenance.

3.4.2.3.4.3 Shall manage the transfer of IT hardware from the AFPOA Data Center from the loading dock.

3.4.2.3.4.4 Shall provide and review technical solutions on a routine basis. The contractor shall analyze technical solutions and assist in preparing implementation plans pertaining to electrical and Data Center HVAC requirements of IT hardware.

3.4.2.3.4.5 Shall act as the point of contact for all hardware installation/relocation and discontinuance of IT equipment. The government will make the determination of what hardware will be discontinued.

3.4.2.3.4.6 Shall create and maintain current Data Center floor plans drawing using AutoCad software.

3.4.2.3.4.7 Shall ensure Data Center site preparation (electrical cables and plugs, cooling, floor panel cable access) for IT equipment hosted at the AFPOA Data Center. The contractor will coordinate with Civil Engineers to request any new electrical cables and plugs.

3.4.2.3.4.8 Shall provide delivery and pre-staging activities for IT hardware.

3.4.2.3.4.9 Shall coordinate with Civil Engineers, vendor and users on any operational maintenance to the Data Center.

3.4.2.3.4.10 Shall monitor the AFPOA Data Center temperature and humidity levels to ensure that standards are maintained. The contractor shall monitor temperature and humidity level machines at least two times per work day. The contractor shall maintain 95% compliance of Review the Temperature and Humidity machine graphs output in the AFPOA Data Center.

3.4.2.3.4.11 Shall initiate and monitor the AFPOA Data Center operational maintenance actions.

3.4.2.3.4.12 Shall coordinate Data Center facility scheduled and unscheduled outages with AFPOA and civil engineers.

3.4.2.3.4.13 Shall provide the security monitoring for the AFPOA Data Center, receiving requests for access and generating/creating/coding access cards.

3.4.2.3.5 Backup and Recovery Administration support: The contractor shall provide Backup and Recovery Administration Journeyman level support to the Swing and Mid shifts, 7 days per week, 365 days per year on-site support to include holidays. Swing Shift runs 1500-2300 CST and Mid Shift runs 2300-0700 CST. The contractor:

3.4.2.3.5.1 Shall monitor approximately 3,000 scheduled weekly backup jobs of UNIX-based and Windows-based operating systems and all related equipment in Data Center, optical storage juke boxes, disk arrays, clustered servers, virtual servers, NetApp NAS, VTL and an automated tape cartridge silo.

3.4.2.3.5.2 Shall accomplish daily, weekly, and monthly backups of databases and operating/file systems utilizing CommVault Simpana software and EMC DataDomain or any other available tools or software purchased by AFPOA. Backups and restores are performed on a routine basis.

3.4.2.3.5.3 Shall perform full and incremental backups of applications user files and databases and their transaction files as required by the customer using vendor’s manuals, documented instructions or trouble shooting procedures with assistance from system administrators or DBAs, on a routine basis.

3.4.2.3.5.4 Shall initiate UNIX commands/shell scripts using documented instructions or troubleshooting procedures as required backup, shutdown databases or rebooting individual servers.

3.4.2.3.5.5 Shall maintain full and incremental backups for an appropriate time period as determined by the needs of the customer and regulatory requirements of the data.

3.4.2.3.5.6 Shall manage and maintain a library of magnetic and /or optical backup media ensuring a complex rotation of media is followed and the correct media for each backup are scheduled for rotations to and from remote storage using documented instructions or trouble shooting procedures as required.

3.4.2.3.5.7 Shall manage and store optical and magnetic media in support of backing up and restoring various systems.

3.4.2.3.5.8 Shall perform as System Administrators on servers and related equipment to ensure operation is stable and continuous.

3.4.2.3.5.9 Shall use the HPOM software suite and other tools that may be available or become available for use to monitor and identify servers that are experiencing problems during non-core duty hours.

3.4.2.3.5.10 Shall identify system failures and equipment problems and take appropriate action according to operational instructions or vendor operating manuals within predetermined time frames. Servers that report critical or major error messages shall be remanded within 15 minutes of detection. This means that some action must be started to resolve the problem within the stated 15 minutes. The contractor shall maintain 95% compliance of annotating HPOM of the initial corrective action taken within 20 minutes of a reported critical or major error messages.

3.4.2.3.5.11 Shall configure, manage, and maintain all hardware and software utilized to control backup storage devices, including drives, libraries, media and clustered server environments, including software patches and firmware upgrades.

3.4.2.3.5.12 Shall document and advertise known defects, quirks, tips, tricks and techniques useful in troubleshooting, configuring, managing and maintaining hardware and software utilized in the daily operation of the Backup and Recovery Environment in the form of TTPs.

3.4.2.3.5.13 Shall respond to customer trouble calls and take appropriate action within 30 minutes on a routine basis.

3.4.2.3.5.14 Shall monitor organization virtual office inboxes for system action notifications and for requests every half hour.

3.4.2.3.5.15 Shall provide management with a report from each shift that provides a status of all backups and restores scheduled via web reporting, hardware, and software problems reported to the vendor. A status shall also be provided on any unscheduled backups and restores.

3.4.2.3.5.16 Shall annotate the Daily Operations Activity Report provided by the government to identify servers experiencing problems and actions taken by the system administrator to resolve the problem. The contractor shall annotate any action taken to call out the vendor, or another point of contact, in the report. The contractor shall log any HPOM notifications owned or annotated and any unusual occurrences taking place in the Data Center floor shall be included in the Daily Operations Activity log shift turnover comments.

3.4.2.3.5.17 Shall provide a smooth handover from one shift to the next. The contractor shall ensure that any problems existing when the shift changes be relayed to the next shift. Shift turnovers shall consist of an informal briefing from one shift to the next.

3.4.2.3.5.18 Shall monitor the AFPOA Data Center temperature and humidity levels during the Swing and Mid shifts to ensure that standards are maintained. The contractor shall report to the appropriate government representative when the temperature and humidity levels are not within standards.

3.4.2.3.5.19 Shall maintain physical security of the data center by confirming all the data center access doors are closed and secure during the Swing and Mid shifts.

3.4.2.3.6 Requirements & Technical Solutions: The contractor:

3.4.2.3.6.1 Shall review applicable requirements and assist the Government in preparing technical solutions and implementation plans.

3.4.2.3.6.2 Shall create, modify and maintain shell scripting to automate Windows System Administration tasks and functions.

- ***Deliverable #32: Shell Scripting Report***

3.5 Cybersecurity and Software Management Support: Contract Personnel performing Security Certification Phase, Security Accreditation Phase, and Continuous Monitoring Phase; A&A documentation support, to include assembling, developing, compiling, or submitting Assessment and Authorization documentation; and having no administrative privileges are designated under DOD 8570.01-M as Information Assurance Workforce Improvement Program (IAM)- Level I (http://www.dtic.mil/whs/directives) and AFMAN 17-1303, Cybersecurity Workforce Improvement Program, May 2016 (http://www.e-publishing.af.mil). Personnel shall have expertise in preparing, monitoring, controlling and processing written and electronic communications from creation to final disposition. Electronic communication will primarily be through email and established electronic workgroup areas (i.e., SharePoint). Written documentation shall be provided as a quality product with minimal editorial changes required. Personnel shall have expertise in project management and delivery of complex tasks (work-breakdown-structures) to meet published timelines as defined within applicable project plans.

Personnel shall have expertise in utilizing the Microsoft Office Suite of applications and Microsoft Visio for developing and editing technical documentation. Personnel shall store all documents created for the task on the appropriate restricted shared drive. No task documents created by the contractor shall be stored on the contractor's issued PC or laptop. The contractor will comply with the filing folder and document naming conventions on the restricted drive. contractor personnel are required to have DoD IA Workforce certifications when initially reporting for duty to the task and maintain the appropriate certification level at all times while working on the task. Contractor personnel who do not maintain certifications shall be denied access to DOD information systems for the purpose of performing information assurance functions and not be allowed to perform on the task.

Senior level A&A personnel shall have at a minimum 5 years of information systems security experience, specifically associated with system accreditation/authorization work which may include RMF, DIACAP or a combination of those processes. Junior level A&A personnel shall have at a minimum 3 years of information systems security experience, specifically associated with system accreditation/authorization work which may include RMF, DIACAP or a combination of those processes. Both levels require IA Workforce certifications. Contractor personnel assigned to this associated task shall maintain a valid Secret security clearance. The contractor must be able to be issued a SIPR token for use on the SIPRNet and be willing to sign a Non-disclosure Agreement (NDA).

The contractor shall be responsible for training contract employees on cybersecurity/IT in the event new technology in hardware or software is implemented at the direction of the government. The training times and dates shall be coordinated with the government representative or the contracting officer before being scheduled.

The Software Management contractor position shall have at a minimum 3 years of Information Technology experience and 1 year testing experience which may include tools like Wireshark, MKRuntest and/or a combination thereof using similar tools or applications. Personnel must have basic knowledge of the RMF or DIACAP process or a combination thereof as well as knowledge of the NIST, Common Criteria, AFNIC and DISA certification programs. The contractor must have the ability to handle multiple certification initiatives and or projects simultaneously and proactively manage each initiative in accordance with established AFNIC processes within established timelines. Contractor personnel assigned to this position shall maintain a valid Secret security clearance. The Software Management contractor position requires the individual to have and maintain an IA Workforce certification to perform administrative-level actions and must be able to maintain an administrative account for testing in accordance with DoD Directive 8570.01-M, IAT Level II.

*****Loss of required certification(s) will result in immediate removal from the task. The contractor will provide a fully qualified replacement as soon as possible, but no later than 30 days from certification expiration.***

The DoD and the Air Force follows the RMF A&A process based on National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems, and NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations (NIST Publications www.CSRC.NIST.gov/publications, to get most current version). A listing of applications/systems with identified scoping information to determine level of effort applicable to the A&A portion of this PWS is provided in Appendix A5.

The contractor shall support the Cybersecurity and Software Management tasks:

- Task Lead
- A&A Project Management
- A&A Package Support
- POA&M Support
- Continuous Monitoring
- Software Management

3.5.1 Task Leader: The task leader: The contractor shall provide an on-site Task Leader for the A&A and software management support tasks. In addition to accomplishing A&A analysis duties, the task leader shall provide leadership, training and management oversight of the contractor personnel assigned to the AFPOA Cybersecurity Division. The task leader shall assign and oversee the execution of the A&A, software certification, and software license management tasks. The task leader shall ensure that the MSR is submitted each month.

3.5.2 A&A Project Management: The contractor shall provide project management services for the A&A task**.** The level of effort required to accomplish the A&A tasks depend upon:
(a) the size and complexity of the information system;
(b) the security category of the system;
(c) the security controls employed to protect the system;
(d) the specific methods and procedures used to assess the security controls in the system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome; and
(e) assessing and evaluating security requirements for each assigned application/system in accordance with the latest guidance governing the Air Force RMF A&A process (AFI 17-101, *RMF for Air Force Information Technology*; (http://www.e-publishing.af.mil)), and AF and DoD accepted software certification processes.

3.5.2.1 A&A and Software Management Support Project Plan (PP):

3.5.2.1.1 The contractor shall provide a draft project plan within 3 business days following the assignment of each task. The PP shall provide at a minimum details surrounding the specific tasks, milestones, delivery schedule, submission dates, and plan for tracking progress and the execution of the A&A; annual security assessments/reviews and software management tasks. Changes to the project plan must be approved by the government lead prior to implementation.

- ***Deliverable #33: PP***

3.5.2.1.2 Shall provide PP updates each week on the day and time as defined by the Government. Updates shall include changes to estimated completion dates, percentage of completion for each task and any issues that could impact task completion.

3.5.2.1.3 Shall meet delivery schedule or coordinated suspense date for the project plan with no more than 3 errors in the document requiring correction.

Shall meet delivery schedule or coordinated tasked suspense's with no more than 3 revisions to documents reporting changes to the AFPOA Information System Security Manager (ISSM) and subsequently to the AO to support an A&A decision.

3.5.3: A&A Package Support: The contractor:

3.5.3.1 Shall build the system A&A package using the current Air Force approved automated tool; currently the Enterprise Mission Assurance Support Service (eMASS). The contractor shall have the ability to use the following A&A automation tools: eMASS, Assured Compliance Assessment Solution (ACAS) and Security Content Automation Protocol (SCAP).

- ***Deliverable #34: A&A Package***

3.5.3.2 Shall assist in the Information System Categorization process and creation of the STIG Applicability List using the Air Force's AFSPC Categorization, STIG, and Assessment Tool (ACSAT) or other method based on Committee on National Security Systems (CNSS) Instruction No. 1253, Security Categorization and Control Selection for National Security Systems (https://www.cnss.gov/CNSS/issuances/Instructions.cfm), and Federal Information Processing Standards Publication (FIPS PUB) 199 (https://csrc.nist.gov/publications/detail/fips/199/final), Minimum Security Requirements for Federal Information and Information Systems (http://csrc.nist.gov/publications/PubsSPs.html), as a part of the RMF activities for each application or system during their performance of A&A for these systems. Deliverables: Security Categorization Document and STIG Applicability List.

3.5.3.3 Shall assist in the selection of common security controls and the preparation of a comprehensive Security Plan to support a continuous monitoring strategy IAW NIST SP 800-37, "Guide for Applying the Risk Management Framework to Federal Information Systems"(http://csrc.nist.gov/publications/PubsSPs.html).

- ***Deliverable #35 Security Categorization Document***
- ***Deliverable #36 STIG Applicability List***

3.5.3.4 Shall provide System Security Plan (SSP) Support. The contractor shall identify the overlays to apply the appropriate security controls to the system and shall document the implementation of these controls in the SSSP IAW NIST SP 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations", and NIST SP 800-53A, "Guide for Assessing the Security Controls in Federal Information Systems and Organizations, Building Effective Security Assessment Plans" (http://csrc.nist.gov/publications/PubsSPs.html).

3.5.3.4.1 The SSP provides an overview of security requirements for the information system and describes the security controls in place or planned for meeting those requirements. The plan can also contain as supporting appendices or as references, other key security-related documents for the information system such as Network Boundary Configuration, Topology, Ports & Protocols System Matrix (PPSM), Users and User Groups, Threat/Risk Assessment, Privacy Impact Assessment (PIA), Contingency Plan, Incident Response Plan (IRP), Configuration Management (CM) Plan, security configuration checklists, and any system interconnection agreements.

- ***Deliverable #37: SSP***
- ***Deliverable #38: Topology, Ports & Protocols System Matrix (PPSM)***
- ***Deliverable #39: Threat/Risk Assessment***
- ***Deliverable #40: Privacy Impact Assessment***
- ***Deliverable #41: Contingency Plan***
- ***Deliverable #42: Incident Response Plan***
- ***Deliverable #43: CM Plan***
- ***Deliverable #44: Security Checklists.***
- ***Deliverable #45:*** *ACAS Scan*

- ***Deliverable #46: SCAP Scan***
- ***Deliverable #47:   Code Scans***
- ***Deliverable #48: PPS Worksheet***

3.5.3.4.2 Shall provide inputs to the approved SSP by updating documents within the contractor's span of control and providing inputs to other/new documents as required.

3.5.3.4.3 Shall support the RMF Team in the assessment of selected security controls required to support the Security Control Assessor (SCA) in preparing a complete Security Assessment Report (SAR). Controls may be identified as Initial Phase (IP) and Final Phase (FP) and all IP controls are required to be answered prior to submission of the ATO package to the AO. FP controls must be fully answered within the first year following the award of the ATO as part of the initial Annual Federal Information Security Management Act (FISMA) Review. The contractor will not fulfill the task if the FP controls are not completed within the first 12 months following the award of the ATO.

3.5.3.4.4 Shall assist in the preparation of a Risk Assessment Report (RAR) containing the results of all security testing, STIGs, and applicable automated vulnerability scans using the AF's tools of choice, currently Assured Compliance Assessment Solution (ACAS) and Security Content Automation Protocol (SCAP) Tools.

3.5.3.4.5 Shall prepare a comprehensive RAR, including mitigations for any unfixable non-compliant findings to determine residual findings and risk that must be addressed and documented within the A&A package.

3.5.4.5.6 PPSM. The contractor shall ensure the system PPSM is registered with the AF PPS Office via the PPS Registration Tool on SharePoint or any other tool as directed by AF PPS Office. Once the system receives a new ATO, the contractor shall update the expiration date of the PPSM using the same tool.

- ***Deliverable #49: RAR***
- ***Deliverable #50: SSP Updates***
- ***Deliverable #51: Network Boundary Configuration***

3.5.4 POA&M Support. The contractor shall provide POA&M support. The POA&M describes the measures that have been implemented or planned:

a) To correct any deficiencies noted during the assessment of the security controls; and
b) To reduce or eliminate known vulnerabilities in the information system.

3.5.4.1 The contractor shall document all identified non-compliant controls and non-applicable security into a POA&M in order to support the submission of the complete Security Authorization Package (System Security Plan, RAR, and POA&M) to the Authorizing Official (AO).

- ***Deliverable #52 POA&M***

3.5.4.2 Upon AO signature of the authorization decision, the contractor shall support continuous monitoring actions for the system and determine impact of any changes to the system and its environment that might generate an update to the A&A package and consideration for reauthorization actions.

3.5.4.3 Shall update the Security Plan, RAR and POA&M to support reporting security status to the AO.

- ***Deliverable #53 SSP, RAR & POA&M Updates***

3.5.4.4 Shall provide advice, recommendations and support for the required decommissioning actions for any system reaching end-of-life.

3.5.5 Continuous Monitoring. The contractor:

3.5.5.1 Shall review and update system security controls according to the AF Information System Continuous Monitoring Guide.

3.5.5.2 Shall provide documentation created for the purpose of the Annual FISMA Review showing that all security controls to be monitored on an annual basis have been reviewed and/or tested and all documents in the System Security Plan have been validated as current or updated as necessary. The system POA&M will be updated accordingly by the contractor. The Annual FISMA Review is due annually no later than the anniversary date of the system ATO during the continuous monitoring years of the ATO award period. If the ATO award is delayed, the Annual FISMA Review will occur but not in the place of the ATO.

- ***Deliverable #54: Annual FISMA Report***

3.5.6 Software Management Support: The contractor shall provide software management support which encompasses two sub-tasks: Software Certification and Software License Management.

3.5.6.1 Software Certification: The contractor shall meet delivery schedules or coordinated tasked suspense's with no more than 3 revisions to the software certification and evaluation testing documentation. The contractor:

3.5.6.1.1 Shall successfully complete the required AF software certification documentation and software testing actions for desktop (to include client/server applications) and web applications; and assist in expediting the software certification processing accomplished by Air Force Network Integration Center (AFNIC). The contractor shall comply with AFNIC's current guidance on Software Certification (https://cs3.eis.af.mil/sites/OO-SC-IA-01/Wiki/Software%20Certification.aspx, (may require login)).

- ***Deliverable #55: AF software certification documentation and software testing actions***

3.5.6.1.2 Shall complete application request worksheets, applicable STIGs, conduct software testing, and ensure compliance with applicable guidance IAW AFI 17-101, *Risk Management*

Framework (RMF) for Air Force Information Technology (IT) (http://www.e-publishing.af.mil) in order to obtain a Certification Decision.

3.5.6.1.3 Shall complete the Application Request Worksheet (ARW) and document application testing results as required on the CM.

- ***Deliverable #56: Applicable Request Worksheets***
- ***Deliverable #57: Application Testing Results***

3.5.6.1.4 Shall complete the software certification package which includes completing the ARW, CM, Ports, Protocols, Services Worksheets and answering all checklist questions.

- ***Deliverable #58: Certification Memo***
- ***Deliverable #59: Software Certification Package***

3.5.1.5.5 Prior to submission to AFNIC for certification consideration, the contractor shall submit software certification package to AFPOA/DFC for review and approval by the Information System Security Manager (ISSM).

3.5.1.5.6 Shall review the validation information for the software (as identified on the ARW) to include vulnerability assessments of any known vulnerabilities, and shall ensure that the software represents a good candidate for software certification testing.

3.5.1.5.7 Upon validation for the software certification process, the contractor shall follow the complete process of tested software evaluation by AFNIC and provide assistance and consultation to AFNIC/NVI as required supporting the final issuance of a software certification decision for the software.

3.5.1.5.8 Shall execute software testing using AFNIC's current checklists. Any implementation documentation specific to COTS products currently available to the government will be provided to the Contractor. If the product is a GOTS product, the contractor shall also conduct a code-scan using Air Force approved certified code-scanning software to verify no vulnerabilities exist within the code, and provide a final report of the code scan with the software certification package.

- ***Deliverable #60: Scan Results Report***

3.5.1.5.9 Upon identification of High and/or Moderate vulnerabilities during testing of an application, the contractor shall notify the ISSM of the vulnerability within 1 business day and provide a mitigation plan. The mitigation plan shall be submitted within 3 business days upon vulnerability discovery and shall include the milestones and estimated completion dates.

- ***Deliverable #61: Mitigation Plan***

3.5.1.5.10 Shall work with the software vendor, AFPOA technicians and Mission Partners to mitigate the finding(s) to the lowest level possible. Finding and mitigation results must be provided to AFPOA/DFC in writing, and documented on the CM for the application.

3.5.1.5.11 Shall use websites identified in the most current Application Request Worksheet (ARW), currently block 4.1 of ARW v3.4, to verify if any vulnerabilities exist within the application. This information can be found on the Air Force Network Integration Center's (AFNIC) Software Certification page at: https://cs2.eis.af.mil/sites/10007/sc/SitePages/Home.aspx .

3.5.1.5.12 Shall work/coordinate with representatives from the AFPOA Cybersecurity Branch in preparing certification packages for submission of information assurance (IA)/IA-enabled software/hardware to National Information Assurance Partnership (NIAP) for Common Criteria certification.

3.5.1.5.13 Shall support the application sponsor (or program manager), Software License Manager and Contracting Officer's Representative in responding to any questions, attending meetings, and/or any other activities/tasks facilitating the development of the certification documentation.

3.5.6.2 Software License Management. The contractor:

3.5.6.2.1 Shall support software license management functions of AFPOA IAW AFMAN 17-1203, *Information Technology (IT) Asset Management (ITAM)* (http://www.e-publishing.af.mil) which would include applications, license agreements, and software upgrades.

3.5.6.2.2 Shall support 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.

3.5.6.2.3 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.

3.5.6.2.4 Shall support common practices for ordering assets, tracking orders and assets, and tagging the assets.

3.6 Lifecycle Management Support: The contractor shall provide support for the following Lifecycle Management tasks:

- Enterprise Architecture
- Equipment Control Officer

3.6.1 Enterprise Architecture (EA): AFPOA EA utilizes Business Process Modeling (BPM) to capture business processes of the AFPOA enterprise in order to analyze current process, support documentation requirements for other processes, train personnel and make improvements to processes. AFPOA uses UNICOM System Architect environment to develop models at all levels of architecture (Operational, Solution Based, Domain Architecture, and Initiative level Architecture) in the DOD Architecture Framework (DoDAF) DoDAF Architecture v2.02 as described in http://dodcio.defense.gov/Library/DOD-ArchitectureFramework/ & DOD Information Enterprise Architecture (DOD IEA) as well as Business Process Model and Notation (BPMN) to enable the integration of Human Resource (HR) business processes across the enterprise. This includes; tracing artifacts to higher levels of architecture such as the Deputy Chief Management Officer (DCMO) Business Enterprise Architecture (BEA), reacting to external factors such as changes in law, updates and replacement of legacy systems and the integration of capability to support Total Force and the ability to analyze, understand, and leverage opportunities afforded by emerging technologies.

3.6.1.1 Shall develop and maintain the current 1559 AFPOA EA models and any future architecture models required to support AFPOA and the AFPOA requirements process.

- ***Deliverable #62: AFPOA EA Models***

3.6.1.2 Shall develop and maintain the AFPOA portfolio capability development roadmaps depicting the major delivery efforts anticipated or underway in and/or impacting the AFPOA Domain.

- ***Deliverable #63: AFPOA Portfolio Capability Development Roadmaps***

3.6.1.3 Shall provide Business Process Modeling (BPM) support to internal AFPOA support activities and analyze, identify and incorporate updates to guidance, policies, and procedures into the AFPOA business processes.

3.6.1.4 Shall coordinate and review the BEA and BPR compliance submissions and facilitate resolution of compliance issues supporting annual funding certifications.

3.6.1.5 Shall submit AFPOA Architecture to the EA Configuration Control Board (EACCB) for review and approval of architecture content for inclusion in AF/A1s repository's production environment.

3.6.1.6 Shall participate in regular EACCB review of architecture content being considered for changes and/or promotion to the production environment of the AF/A1 EA shared repository.

3.6.1.7 Shall facilitate a review of architecture for promotion from the repository's development environment to its production environment. The contractor shall review architecture to ensure compliance with established standards, conventions, and structure. The contractor shall produce/brief review findings as required.

3.6.1.8 Shall manage and maintain the AFPOA encyclopedias, to include version control, migration, and archiving of the AFPOA architecture products.

3.6.1.9 Shall develop RMF artifacts to support ATO packages.

- ***Deliverable #64: RMF Artifacts***

3.6.1.10 Shall maintain awareness of AF and DOD strategy and plans for structure to support enterprise architecture and requirements toolsets.

3.6.1.11 Shall recommend and document courses of action that may include migration/transition of the central repository to other environments, software, or service platforms.

- ***Deliverable #65: Courses of Actions***

3.6.1.12 Shall review and recommend response to information support plans impacting the AFPOA Domain.

3.6.1.13 Shall attend EA related working groups, forums, and meetings to remain informed and engaged on latest activity, policies, and procedures.

3.6.1.14 Shall inspect compliance fields in the Information Technology Investment Portfolio System (ITIPS): pass data, list of interfaces, what BEA version asserted to, and BEA compliant.

3.6.1.15 Shall complete Weekly Activity Report detailing all activities and accomplishments for the week and meet delivery schedules or coordinated tasked suspense.

3.6.2 Equipment Control Officer (ECO): The contractor shall provide an ECO that is responsible managing all accountable IT assets utilized by AFPOA personnel as daily Office Automation (OA) equipment as well as the enterprise systems. All Asset Management activities will be executed IAW AF guidance to include AFMAN 17-1203 "IT ASSET MANAGEMENT (ITAM)" and AFI 23-111 "Management of Government Property in Possession of the Air Force. The ECO will be functionally aligned under the AFPOA Lifecycle Management Division AFPOA/DFL. The ECO will have the ability to react to changes in external factors such as advances in OA technology as well as large scale changes to the AFPOA Data Center. The contractor:

3.6.2.1 Shall be appointed by the AFPOA Director to perform as the AFPOA Equipment Control Officer in accordance with AFMAN 17-1203 section 1.2.11 with the exception of all inherently governmental functions in accordance with Federal Acquisition Regulation (FAR) Subpart 7.5, "INHERENTLY GOVERNMENTAL FUNCTIONS."

3.6.2.2 Shall provide overall management of IT assets to include local storage and distribution of IT property as well as leveraging emerging technologies by developing strategic plans for the lifecycle management of the AFPOA fleet of OA equipment.

3.6.2.3 Shall develop IT Refresh plan for all organizations supported Standard Office Automation equipment to include desktops/laptops, monitors and multi-function printers etc.

- ***Deliverable #66: IT Refresh Plan***

3.6.2.4 Shall plan, develop and execute deployment plan for strategic refresh (desktops, laptops, monitors and printers) annually.

- ***Deliverable: #67 Deployment Plan***

3.6.2.5 Shall manage the local IT storage area.

3.6.2.6 Shall schedule necessary equipment logistics – Disposal Services and 502nd CS. Vehicle and operator will be provided by the Government and will be made available for scheduling with one week notice.

3.6.2.7 Shall track status and provide ad hoc reporting of status of all equipment.

- ***Deliverable # 68: Report***

3.6.2.8 Shall work with existing AFPOA Property Custodians and provide help with the management and inventory of all AFPOA assets.

3.6.2.9 Shall work to identify excess IT equipment and notify PCs for turn in.

3.6.2.10 Shall harvest, store and issue usable equipment as well as process and dispose of unusable equipment

3.6.2.11 Shall receive, store and reissue IT accessories such as keyboards, mice, Common Access Card (CAC) readers, speakers, microphones, cables and other non-accountable peripherals).

3.6.2.12 Shall recommend and document courses of action that may include migration/transition to new technology or ways of doing business.

3.6.2.13 Shall attend meetings, working groups and forums, to remain informed and engaged on latest activity, policies, and procedures within AFPOA and to support leadership.

Factor	**Data**
Code and data complexity	Include the following types of information: Number of code modules by type (i.e. C, Java, JSP, PL/SQL, TCL/TK, C#, COBOL, 4GL, Pearl, etc.) Number of reusable modules (i.e. COBOL copy book elements, C library modules, Java utility classes/libraries, Screen/HTML templates, XML modules, JCL, Unix scripts, Screen resource elements, Stored Procedures, SOA web services, etc.) Number of online screens. Number of report programs (if using COTS BI/Ad Hoc Reporting tools, provide the number and types of each module including database table views, joins, Cubes, etc.). Database definitions (i.e. number of tables, number of data elements, number of primary keys, foreign keys, number of table joins,

Factor	**Data**
	etc.). This can be provided in the form of logical and physical data models.
Stability	Provide the Mean Time to Repair on the legacy code. Provide the defect density (the number of defects/DIREPS/SCRs average per Function Point or 1000 Lines of code). This is preferred by the type of code listed in the first row of this table. The average (in FP or SLOC) number of modifications/improvements per period (quarterly, annually, etc.) per Baseline Change Request.
Number of concurrent users	
Application age	
Function Points Inputs External Inputs	
External Outputs	
Logical Internal Files	
External Interfaces	
External Inquiries	
Initial response time	Provide the current average response time for online applications and/or web services. Provide the expected/desired response time for online applications and/or web services. If there are throughput requirements on batch/background updates or reports, provide the current average and the desired goal/objective.
Life expectancy	

Factor	**Data**
Operating system	Provide a complete list of the OS and all COTS/GOTS utilities including Development Tools along with the version numbers of each.
Platform	Provide the list of the HW baseline for servers along with capacity, model numbers, etc.
Programming Languages	See first row above. Also provide the programming language versions being used (i.e. Java 1.6, TCL/TK 8.4.x, COBOL 85, Oracle 11G, etc.)
Programs	See row 1 above. This need to be expanded to show the profile of all the types of development components (i.e. copy books, libraries, JCL, scripts, screen definitions, etc.) and not just the number of programs.
Database	See row 1 above on the database information needed.
COTS	Provide complete list and version numbers. Also provide any licensing restrictions/limitations that my prohibit exploitation by a bidder on the use of a product that is limited for that application/project.
Avg. transactions per day	This needs to be by type (i.e. updates, inquiries, web services, etc.).
Interfaces	Provide ICDs or equivalent information about the nature and design of the interface (i.e. frequency, data definitions, triggers, mechanism such as ftp or web service, etc.).
Upgrades	Planned as well as past history for both COTS and the applications.
Average help desk call volume	Provide by severity levels and the numbers that have passed from level 1 to 2 to 3.