PERFORMANCE WORK STATEMENT

PROJECT TITLE:
Automated Funds Management System Standard Financial Information Structure Compliance and Sustainment

TASK ORDER TYPE:
Hybrid (Firm Fixed Price and Labor Hours)

1 Introduction

1.1 Purpose

The Business Enterprise Architecture (BEA) is the enterprise architecture for the Department of Defense (DoD) Business Mission Area and reflects DoD business transformation priorities; the business capabilities required to support those priorities; and the combinations of enterprise systems and initiatives that enable those capabilities. It also supports use of this information within an End-to-End (E2E) framework.

The purpose of the BEA is to provide a blueprint for DoD business transformation that helps ensure the right capabilities, resources and materiel are rapidly delivered to our warfighters – what they need, when they need it, where they need it, anywhere in the world. The BEA guides and constrains implementation of interoperable defense business system solutions as required by the Section 2222 of Title 10 United States Code. It also guides information technology investment management to align with strategic business capabilities as required by the Clinger-Cohen Act, and supports Office of Management and Budget (OMB) and Government Accountability Office (GAO) policies.

The Standard Financial Information Structure (SFIS) is a comprehensive data structure that supports requirements for budgeting, financial accounting, cost/performance, and external reporting needs across the DoD enterprise. SFIS standardizes financial reporting across DoD and allows revenues and expenses to be reported by programs that align with major goals, rather than basing reporting primarily on appropriation categories. It also enables decision-makers to efficiently compare programs and their associated activities and costs across the department and provides a basis for common valuation of DoD programs, assets, and liabilities.

This Performance Work Statement (PWS) defines the requirements for non-personal technical support services for the SAF/FMF Air Force Financial Systems Office (AFFSO) Wright-Patterson Air Force Base (WPAFB), OH. The Contractor shall function as a single focal point to the Government for modifications to the Automated Funds Management (AFM) System required to comply with the BEA, SFIS and integrate with Air Force (AF) Enterprise Resource Planning (ERP) efforts. In addition the contractor shall function as a single focal point to the Government for the maintenance, sustainment, and enhancement activities for the as-is and to-be versions of AFM. The contractor shall:

- Design, code, unit test, formal test, and implement AFM BEA/SFIS requirements.
- Provide software maintenance, enhancement and sustainment support for the fielded version of AFM.
- Develop train-the-trainer training for AFM.
- Maintain end user training materials for AFM.
- Provide second and third tier Help Desk support for the functional and technical user community.
- Operate, maintain, and administer computer hardware, operating system (OS), Database (DB), Web-Server (WS), and utility software.

1.2 Program Status

The AFM system is a web-based, real-time, enterprise system for the Funds Control, Funds Management, and Funds Distribution processes of the AF at the Air Staff and Major Command (MAJCOM) levels. AFM is designed to assist AF financial managers by automating funds control, management and distribution of appropriated funds at the maximum amount allowed by law down to the installation level. The Defense Finance and Accounting Service (DFAS) initiated development of Standard Fiscal Code (SFC) for standardized coding of financial transactions that would be common across all services and all phases of the budget cycle. AFM was one of the first systems designed to use SFC to be replaced by the SFIS in the future.

The data element tables and descriptions found within AFM are compliant with the SFC structure with legacy data elements maintained for backward compatibility. The SFC structure is similar to SFIS but changes to data element names and sizes are required along with adding new data elements. These changes will affect business rules, the database, user interface, reports, and system-to-system interfaces.

1.3 Program Summary

AFM uses a Sun Solaris 10 platform. Sun Solaris 10 is open architecture and easily reads other data systems files and has the ability to export/interface data to/from other systems. ORACLE is the relational database management system (RDBMS) employed by AFM. RDBMS was chosen to provide users with maximum data access through flexible reports and data file construction and generation. AFM's ad hoc reporting tool is custom developed and embedded within the user interface. The following table summarizes AFM's system specifications.

Factor	AFM Specification	Factor	AFM Specification
Code and data complexity	330+ Java programs 340+ JSP files Approximately 110 PL/SQL programs 12+ External Java Libraries 20+ JavaScript Libraries/Plugins 180+ Online screens 45 report programs. 170+ Database Tables 100+ Database Triggers 50+ Database Views	Operating system	Solaris 10 x86-64 Symantec Netbackup 7.6 Common Array Manager 6.9 Open Text Xceed 15 Wireshark 1.14 PL/PDF 2.7.0 SQLDeveloper 4.0.3.16 Oracle WebLogic Server 12.1.1.0
Stability	The system has been in sustainment for eleven years and as such, is a stable program. The average number of fixes and/or improvements per quarter can run anywhere from 1 to 6. The average number of fixes to the as-is version of AFM is one major modification and 6 to 8 minor changes per year.	Platform	2x Sun FIRE X4470 M2 128 GB RAM 5 TB disk storage 8 NIC ports Attached to SAN via SAS 1x Sun FIRE X4170 M2 24 GB RAM 1 TB disk storage 2 NIC ports Attached to robotic tape library 4x Oracle v40z 8 GB RAM

			600 GB disk storage 2 NIC ports 1x SL500 2x LTO5 drives 3x StorageTEK 2530-M2 2x StorageTEK 2501 3x Storageteck 2540
Number of concurrent users	600 active users, number of concurrent users varies. 50+ handled with no problems.	Programming Languages	Java 1.7 Servlet 3.0 JSP 2.2 PL/SQL 12.1.0.1.0
Application age	14 years	Database	Oracle 12.1.0.1.0 TNS for Solaris: 12.1.0.1.0 NLSRTL 12.1.0.1.0
Initial response time	The response time is near instantaneous. Response times can vary based on the amount of information queried, saved, or uploaded.	Avg transactions per day	2600+
Interfaces	ABIDES - 1 inbound file CRIS – 1 outbound file DEAMS - 2 outbound files EFD - 5 outbound files FMSuite – 1 inbound and 2 outbound files. GAFS-R - 3 outbound files.	Average help desk call volume	Approximate Monthly Average: Total - 160 Resolution at: Level 1 – 4 Level 2 – 150 Level 3 – 6

2 Scope

2.1 General Scope of Work

The Contractor under this Performance Work Statement shall provide the necessary services, and products to deliver a turn-key fully operational BEA and SFIS compliant AFM system. These services shall include maintenance, operation, sustainment, and enhancement of the non BEA/SFIS version of AFM currently fielded.

The range of services to be procured under this PWS shall include:

- Providing Tier 2 and Tier 3 help desk support.
- Planning, managing and performing tasks such as coordinating technical interchange meetings with systems owners, users, and operations and maintenance entities to identify gaps, gather, decompose and allocate requirements to functions, and catalog these requirements. Perform

analysis and present formal reports comparing contractor gathered requirements with the government provided preliminary requirements.

- Providing solutions fully compliant with Federal statutes, regulatory accounting standards, and other emerging requirements uncovered during this project.
- Migrating the as-is version and developing the BEA/SFIS version to an operating system that is compatible with cloud computing such as RedHat Linux.
- Eliminating and replacing PLPDF generated reports and documents with another software package.
- Designing, developing, and delivering engineering architectures, baselined software code, licenses, and operational systems that compose AFM.
- Presenting the Contractor's management strategy, including an Integrated Master Schedule (IMS) for procuring or building software modules, transferring licensing to the government, identifying ports and protocols of applications for Information Assurance (IA) certification purposes, ensuring modules or application deliveries are on schedule.
- Designing and implementing configuration management processes and methods compatible with Air Force configuration and change management policies.
- Identifying Net Ready Key Performance Parameters (NR-KPP) for qualification, government acceptance, and Joint Interoperability Test Command (JITC) Interoperability Certification testing.
- Performing all requisite actions required to host the BEA/SFIS and existing versions of AFM in a cloud computing environment.
- Planning, coordinating and delivering finished products by performing module and integration level development, qualification acceptance, and government acceptance tests.
- Producing artifacts and acquiring Information Assurance certifications using the Risk Management Framework (RMF).
- Providing systems engineering, and Information Systems Security Officer (ISSO) staff support.
- Developing and providing systems documentation, knowledge base articles, training presentations, and manuals for training the trainer and users.
- Supporting the ongoing process and system changes to enable the Air Force to meet its Chief Financial Officer (CFO) Information Technology (IT) compliance, Financial Improvement and Audit Readiness (FIAR), Federal Information Security Management Act (FISMA), and Financial Information System Control Audit Manual (FISCAM) requirements.

3 Quality

Both the contractor and Government have responsibilities for providing and ensuring quality services.

3.1 Quality Control

The contractor shall establish and maintain a complete Quality Control Plan (QCP) to ensure the requirements of this PWS are provided as specified in accordance with the applicable Inspection of Services Clause. The contractor shall make appropriate modifications (at no additional costs to the government) and obtain acceptance of the plan by the contracting officer (CO). The Government has the right to require revisions of the QCP should the incorporated plan fail to deliver the quality of the services provided at any time. The plan shall include, but is not limited to the following:

A description of the inspection system covering all services listed.

- The specification of inspection frequency.
- The title of the individual(s) who shall perform the inspection and their organizational placement.
- A description of the methods for identifying, correcting, and preventing defects in the quality of service performed before the level becomes unacceptable.
- On-site records of all inspections conducted by the Contractor are required. The format of the inspection record shall include, but is not limited to, the following:
- Date, time, and location of the inspection.
- A signature block for the person who performed the inspection.

- Rating of acceptable or unacceptable.
- Area designated for deficiencies noted and corrective action taken.
- Total number of inspections.

3.2 Quality Assurance

The Government will perform periodic reviews of the contractor's performance in accordance with the Government's Quality Assurance Surveillance Plan (QASP). The Government reserves the right to review services to be provided, including those developed or performed at the Contractor's facilities, to determine conformity with performance and technical requirements.

4 Primary Performance Objectives

The tasks described in this section identify known activities the Contractor may be required to perform in support of AFM. The Contractor shall provide products in execution of the mission in the areas of financial management, acquisition management, logistics management, engineering, test and evaluation, configuration management, Government property management, administrative, technical data management, help- desk support and procurement management support. Work for these efforts may be assigned to be accomplished either on-site at the Contractor's facility for the Sustainment effortor off-site at the Government facility for the BEA/SFIS effort..

4.1 Program Management

The Contractor's Program Planning, Project Monitoring and Control, Configuration Management (CM), Process and Product Quality Assurance, and Risk Management processes shall be conducted using no less than level 3 Carnegie Mellon University Software Engineering Institute (SEI) Capability Maturity Model Integration (CMMI). The Contractor's Program and Project Planning and Control shall include Scheduling, Technical Performance Metrics, CM, Quality Assurance (QA), Risk Management, and Change Management (CM). The contractor shall use standard tools and the Financial Management (FM) Information Technology Lifecycle Management (ITLM) tool suite. The SAF/FM ITLML tool suite includes:

- Serena Business Manager for Help Desk Support, Incident Management, and System Change Requests.
- Serena Dimensions for Configuration Management.
- Microsoft Project Server for scheduling.
- IBM System Architect for architectural artifacts.
- IBM Rational DOORS for requirements analysis.

These tools will be hosted and operated by the Government.

4.1.1 Integrated Management Plan

The Contractor shall generate and maintain an Integrated Management Plan (IMP) that provides the measurable, event-oriented approach to planning, managing, and controlling all technical aspects of the AFM task order. The IMP shall identify and describe:

- Key project events.
- Tasks required to achieve each project event.
- Criteria for entering and/or exiting the tasks.
- Risk management.
- Assignment of functions, duties, and responsibilities.
- Management procedures, policies, reporting requirements; and methodology for accomplishing contract tasks.

The IMP shall be the basis for development projects and plans and shall provide an informative structure on the relationship of quality assurance plans, project plans, configuration management plans, risk management plans and any other documents guiding program or project-level processes

and procedures. It shall be updated as required to reflect changes in the program and the defined processes

4.1.2 Integrated Master Schedule

The Contractor shall develop and maintain an Integrated Master Schedule (IMS) to manage the contractually authorized work for each release. All scheduled work elements shall be integrated into the IMS, including all stakeholder groups within the AFM program office, and the Contractor's development team. The schedule shall be constructed as a logic-network employing Critical Path Methodology (CPM) and shall identify all activities, constraints, milestones, Contract Data Requirements List (CDRL) deliverables, and resource requirements. The schedules shall extend to a sufficient level of detail to mitigate risk and measure performance and shall ensure that vertical and horizontal traceability is maintained at all times.

4.1.3 Change Management Plan

The contractor shall review, update, implement, and maintain the AFM Change Management Plan (CMP). The CMP depicts the PMO approved policies and procedures for processing Change Requests (CRs), Defect Reports (DRs), Software Problem Reports (SPRs), and change response documents. The AFM PMO is the approval authority for the CMP.

Software DRs shall be classified and resolved as follows:

- Category 1 – 'Critical': Denotes a problem that prevents accomplishment of essential capability or jeopardizes safety or other requirements designated as 'Critical'. The contractor shall provide a fix or workaround within 48 hours of the DR creation with a maximum of seven 7 days for the fix to be sent to the field.
- Category 2 – 'Major': Denotes a problem that adversely affects the accomplishment of an essential capability or adversely affects cost, technical, or schedule risks to the project or to the life cycle support of the system and no work-around solution is known. For fielded systems, provide a fix/work-around within 45 days of the DR creation.
- Category 3 – 'Average': Denotes a problem that adversely affects the accomplishment of an essential capability or adversely affects costs, technical/scheduled risks to the project or to the life cycle support of the system and a work-around solution is known.
- Category 4 – 'Minor': Denotes a problem that results in operator inconvenience or annoyance but does not affect a required operational or mission essential capability or results in inconvenience or annoyance for development/maintenance personnel, but does not prevent the accomplishment of the responsibilities of those personnel.
- Category 5 – 'Other': Denotes any other effect not covered by any other category definition given previously.

4.1.4 Communications and Information Systems Requirements Document (CSRD)

The PMO will document any development, maintenance, or enhancement requirements to the AFM application on a Communication and Information Systems Requirement Document (CSRD).

4.1.5 Software Development Plan

The contractor shall develop a Software Development Plan (SDP) for each release that details the project plan, including the requirements, level of effort, duration, risks, assumptions, derived requirements, and any associated costs for other direct cost (ODC) purchases. The SDP will be based on the IMP and will document any deviation from the IMP. The SDP will be a living document through the development project and will be used to track changes that occur after a project is baselined.

4.1.6 Preliminary Design Document

On receipt of the CSRD, the Contractor will perform an analysis of the requirements and prepare a Preliminary Design Document (PDD). The approved PDD will describe the high level system change

requirements, proposed program changes, and identify all documentation that must be updated. The Contractor will present the PDD at the Preliminary Design Review (PDR) and once approved will serve as the basis for developing a detailed solution.

4.1.7 Software Design Document

The contractor shall develop a Software Design Document (SDD) to describe the complete design for the Computer Software Configuration Items (CSCI) necessary to implement requirements identified in the PDD. The SDD shall be presented to the government at the Critical Design Review (CDR) and shall describe the allocation of requirements from a CSCI to its Computer Software Components (CSCs).

4.1.8 Software Test Plan

The contractor is responsible for all test activities prior to product delivery and Government Acceptance Testing (GAT). For each release, the contractor shall develop and maintain a Software Test Plan (STP) describing the Contractor's plans and procedures for completing and documenting unit testing, integration testing, regression testing, functional testing and other activities required to support GAT. Functional testing includes the steps necessary to demonstrate that each release satisfies requirements specified in the PDD.

Once GAT begins, any defects encountered shall be documented in a Software Problem Report (SPR). The contractor shall correct the defect and resubmit the software for testing. All critical and major (Category I and II) SPRs will be resolved and retested before GAT is complete. If any category III – V SPRs are not resolved for any reason, they will become DRs and will be logged in Serena Business Manager to be prioritized and fixed in a future release or patch.

4.1.9 Software Test Description

The contractor shall develop Software Test Descriptions (STD) consisting of software test scenarios (STS) and software test cases (STC) capable of testing all development, maintenance, sustainment, and enhancement modifications included in each AFM system release. Further, the contractor shall review, update, and maintain the existing STS and STC library encompassing all aspects of AFM functionality to facilitate timely and effective regression testing.

4.1.10 Software Test Reports

The contractor shall produce Software Test Reports (STR) for each AFM system release. The STR will summarize the results of the contractor's testing effort prior to GAT. The STR will be presented to the Government at a Test Readiness Review (TRR).

4.1.11 Requirements Traceability Matrix

The contractor shall develop and maintain a Requirements Traceability Matrix (RTM) to demonstrate how requirements are satisfied by the design, design specifications are satisfied by the code, and code changes are tested. .

4.1.12 Software Version Description Document

The contractor shall produce a Version Description Document (VDD) for each release. The VDD is the primary configuration control document used to track and control versions of software to be released to the operational environment. It is a summary of the features and contents for the software build. It identifies and describes the version of the software being delivered to the Government, including all changes to the system.

4.1.13 Software Configuration Management Plan

The contractor shall perform formal configuration management of all aspects of AFM. The contractor shall review and update the AFM Software Configuration Management Plan (SCMP) and deliver a proposed SCMP that identifies internal contractor process, tools, and guidelines that align with the

PMO approved CMP within 30 business days after contract start. This SCMP defines guidelines for the process governing deliveries, change requests, delivery defects, problem reports, sustainment, and the deployment steps from contractor delivery to production. The contractor shall implement the SCMP in every software change and documentation change. The AFM PMO is the approval authority of the SCMP.

4.1.14 Program Performance Metrics

The Contractor shall establish, maintain, and use metrics that are appropriate to the authorized scope of work and shall routinely report these to the Program Management Office (PMO). Metrics shall be product-oriented and/or based on performance parameters that are discretely measurable. The Contractor shall also support the PMO in developing and reporting these metrics to other Government personnel. Changes that impact Contractor-delivered metrics shall require prior coordination with the PMO.

4.1.15 Monthly Status Report

The contractor shall deliver a Monthly Status Report (MSR) to summarize all work performed during the previous month. The MSR shall:

- Record resource hours and costs against government defined tasks to support accurate project cost accounting using government formats and tools for the time and materials portion of the contract.
- Status of tasks, schedules, and CDRL deliverables. Status of tasks shall include a summary description and schedule of all tasks completed during the reporting period, all tasks currently on-going during the reporting period, and all known tasks assigned for future reporting periods.
- Current and cumulative task funding status (direct labor, travel, and Other Direct Costs (ODC) funding status to be reported separately.)
- Outstanding issues, and proposed resolution approaches and actions to resolve any outstanding issues.
- Staffing report identifying current staffing roster, all current vacancies, and a record of all staffing departures.
- System Availability Rates.

4.1.16 Risk Management Plan

The contractor shall implement and maintain a Contractor's Risk Management Plan (RMP). The RMP shall describe processes and procedures for identifying, assessing, tracking/monitoring, communicating, and mitigating program and project risks. The RMP shall be initially included as part of the IMP and shall be updated as required.

4.1.17 Information Systems Contingency Plan

The contractor shall review, update, implement, maintain and exercise the existing AFM Information Systems Contingency Plan (ISCP). This ISCP establishes the capability, procedures, and after action requirements to ensure AFM operation during a service disruption. The AFM PMO is the approval authority for the ISCP.

4.1.18 Incident Response Plan

The contractor shall review, update, implement, maintain and exercise the existing AFM Incident Response Plan (IRP). This IRP establishes a response framework for an event or action which may cause or is causing a disruption to the normal operation of the system. The AFM PMO is the approval authority for the IRP.

4.1.19 Information System Security Plan (ISSP)

The contractor in conjunction with other contract and government employees shall review, update, implement, maintain, and exercise the Information System Security Policy (ISSP). The ISSP identifies

procedures and mechanisms that minimize the risk of implementing AFM in an operational environment. This document further provides direction and criteria for using specialized security measures and disciplines during AFM's operational lifecycle. The ISSP will be created and maintained either manually or in the Enterprise Mission Assurance Support Service (eMASS). The AFM PMO is the approval authority for the ISSP.

4.1.20 Information Support Plan

The contractor shall review, update, implement, and maintain the existing Information Support Plan (ISP). The ISP describes information technology needs, dependencies, and interface activity for AFM. It focuses on the efficient and effective exchange of information. The ISP is created, updated, reviewed, and approved using the Global Information Grid (GIG) Technical Guidance Federation (GTG-F) or its successor. The AFM PMO is the approval authority for the ISP.

4.1.21 Department of Defense Architecture Framework Artifacts

The contractor shall review, update, create and maintain Department of Defense Architecture Framework (DoDAF) Artifacts. The DoDAF is the overarching, comprehensive framework and conceptual model enabling the development of architectures required by the Clinger-Cohen Act. The AFM PMO is the approval authority for DoDAF artifacts.

4.1.22 Interface Control

The contractor shall review, update, create, and implement Interface Control Documents (ICD) The ICDs consist of the documented strategy to keep data synchronized between source and target applications. The AFM PMO is the approval authority for the ICDs. Each ICD shall include at a minimum:

- An explanation of each interface.
- Interface method chosen (manual or batch, etc.).
- Data fields being interfaced.
- Controls to reasonably assure that the data is interfaced completely and accurately.
- Timing requirements.
- Definition of responsibilities.
- System balancing requirements.
- Security requirements.

4.1.23 AFM Training Plan

The contractor in conjunction with other contract and government employees shall review, update, implement, and maintain the existing AFM Training Plan. The plan outlines the training activities and collateral support materials required to instruct AFM users on the systems functionality. The AFM PMO is the approval authority for the AFM Training Plan.

4.1.24 Additional Technical Studies and Reports

The contractor shall prepare additional reports, not to exceed five per year, as deemed necessary by the PMO. The studies or reports may include performance studies, analyses, Rough Order of Magnitude (ROM), or Engineering Change Proposal (ECP).

5 Technical Requirements

The PMO, in conjunction with the AFM Functional Requirements Review Board (FRRB) and Configuration Control Board (CCB), shall establish the requirements for software development, maintenance, and enhancement activities. The Contractor shall manage, plan, design, code, test, and develop user manuals and training material for all development, maintenance, sustainment, and enhancement activities.

5.1 BEA/SFIS Compliant Version of AFM

The Contractor shall convert all aspects of AFM to comply with all BEA and SFIS requirements. This includes ensuring transactions are identified and recorded based on their impact to the United States Standard General Ledger. This requirement shall entail application of the system engineering process to include all phases of requirements, design, test, and execution.

The contractor shall work as part of a multi contract and multi organizational team to design, develop, and implement translation services for the BEA/SFIS compliant version of AFM. The BEA/SFIS compliant version of AFM will generate and send all interfaces in SFIS format. Backward compatibility for legacy system interfacing partners will be achieved through a data translation service such as the Defense Logistics Agency's Global Exchange (GEX).

5.2 AFM Maintenance and Sustainment

The Contractor shall perform maintenance and sustainment activities that include designing, coding, testing, and implementing AFM requirements. This encompasses all aspects of operating the production, development, and test environments of AFM. Maintenance and sustainment activities will apply to both the non SFIS version of AFM and the BEA/SFIS compliant version once it is fielded.

5.2.1 Help Desk Support

The contractor shall provide tier 2 and tier 3 help desk support for the fielded version of AFM.

- Tier 2 help desk support entails support for application software and hardware.
- Tier 3 helpdesk support entails subject matter expert support to resolve issues that could not be resolved at the tier 2 level. This normally involves complex issues related to hardware, software and operating system issues.

5.3 System Administration and Database Administration

The Contractor shall maintain all production, development, training, and test environments to conduct AFM development, maintenance, sustainment, enhancement, and production processing. All environments are currently hosted in government facilities but are subject to rehost in a commercial, military, or hybrid cloud solution.

The contractor may be required to maintain two test and development environments, one at the government facility and one at the contractor facility, dependent on the adequacy of using a Virtual Private Network (VPN) connection to the test development environment. If developing over the VPN is problematic the contractor may then be required to ship a server from the Government facility to the Contractor's facility. Government Furnished Equipment will be provided for both environments. The Contractor shall perform general maintenance and system administration required for operating these environments wherever they are hosted.

5.3.1 System Administration

The contractor shall provide System Administration for all environments. The contractor shall be responsible for administering and maintaining the operating system, hardware, and software. Responsibility for hardware may transfer to the cloud service provider in the future. System administration includes:

- Maintaining a production system availability rate of 99.7% or greater except for scheduled maintenance.
- Providing processing capability 24 hours per day, 7 days a week
- Installing, maintaining, upgrading, and migrating hardware, software, and equipment.
- Administering the operating system and webserver.
- Deploying AFM releases.

- Monitoring, analyzing and implementing Time-Compliance Network Orders (TCNO), Information Assurance Vulnerability Management (IAVM) Packages, Critical Patch Updates (CPU), and other remediation activities required to maintain the systems security, integrity, and availability.
- Establishing, tracking, and managing ports, protocols, and services (PPS) within the appropriate PPS Management tools.
- Implementing, integrating, and managing the systems Primary Key Infrastructure(PKI) certificates.
- Implementing and enforcing required Security Technical Implementation Guide (STIG) audit requirements.
- Developing, maintaining, and updating shell scripts.
- Performing network and interface monitoring, management, and troubleshooting.
- Coordinating with the appropriate organizations to resolve network, hardware, or related concerns.
- Scheduling, managing, verifying, and storing full system backups.
- Developing and maintaining AFM documentation for system operations, web server operations, backup and recovery, and system audit plans.
- Performing Restart and Recovery Procedures

5.3.2 Database Operations

The contractor shall provide Database Administration for the AFM system. The contractor shall be responsible for administering, creating, and maintaining all databases required for development, testing, and production usage. Database administration includes:

- Installing database releases, patches, and performing database upgrades and or migrations.
- Performing capacity planning to create and maintain databases.
- Planning and implementing backup and recovery of databases.
- Controlling migrations of programs, database changes, and data changes throughout the development cycle.
- Monitoring, analyzing and implementing Time-Compliance Network Orders (TCNO), Information Assurance Vulnerability Management (IAVM) Packages, Critical Patch Updates (CPU), and other remediation activities required to maintain the systems security, integrity, and availability.
- Implementing and enforcing security for all databases and performing required Security Technical Implementation Guide (STIG) audit requirements.
- Establishing and administering database users and roles.
- Managing and tuning database imports, exports, log files, and objects.
- Monitoring performance, background processes, database views, schema objects, table space, indexes, logs, and synonyms.
- Allocating resources.
- Accessing and analyze cache file utilization and performance.
- Tuning PL-SQL statements, database performance and maintaining stored procedures.
- Creating and maintaining documents depicting database design, operation plans, security plans, and monitoring plans.

5.4 Hardware and Software Management

The contractor shall manage all hardware, software, firmware, related supplies, support agreements, maintenance agreements, and licenses that are integral and necessary for the performance of activities identified in this PWS. Responsibility for hardware may transfer to the cloud service provider in the future.

5.4.1 Hardware and Software Configuration Report

The contractor shall develop and maintain the Hardware and Software Configuration Report for AFM. The report shall include the production, development, and test hardware configurations to the sub-component level, as well as all licensed software and individually licensed products. The report shall

include the license identification and keys for acquired commercial off the shelf software and any other support and maintenance agreements required.

5.4.2 Other Direct Costs

The Government may require the contractor to purchase hardware, software, firmware, related supplies/warranties/ help desk requirements, technical refresh and other support as needed that are integral and necessary for the performance of this task order. ODCs are ancillary in nature and integrally related to the contractor's ability to perform the service being acquired. An ODC must satisfy the criteria expressed within the scope of the task order and must not duplicate costs covered in other areas of the task order.

- ODCs for materials and/or supplies necessary for performance of this task order shall be reimbursed in accordance with the billing and payment clauses of this task order. The Government Contracting Officer will establish a not-to-exceed ODC ceiling and determine the fair and reasonableness of the proposed price/prices. Pursuant to FAR 16.601(b)(2), materials are to be provided at actual cost except as provided for in FAR 31.205-26(e) and (f).
- Prior to acquiring ODCs, the contractor shall submit a request through an action memo to the CO or COR for verification and approval. This request must identify the item(s) to be purchased, estimated cost(s), vendor, and reason for purchase.
- The COR or CO must review the ODC request. If the request is complete and the ODCs are clearly identified in the contractor's quote, the COR or CO may approve the request. In any other situation, the CO must review and approve the request. In some instances, a task order modification may be required to acquire the ODC. In that situation, the ODC may not be purchased prior to award of the modification.

5.5 Cybersecurity, Certification, and Accreditation

The Contractor shall follow the Risk Management Framework (RMF) for DoD Information Technology (IT) process. All system products and activities shall be planned, designed, developed, tested, deployed, sustained, and conducted in accordance with, the Committee on National Security Systems (CNSS), National Institute of Standards and Technology (NIST), Department of Defense (DoD) and Air Force Cybersecurity policy, guidance, and standards. The system shall comply with the most recent versions, amendments, and/or addendums of the statutory and regulatory policy, guidance, or standards. In the event applicable Federal, DoD, or Air Force policy, guidance, or standards change, the contractor will prepare a change proposal to bring the system into compliance.

5.5.1 Personnel Cybersecurity

In accordance with Air Force Manual (AFMAN) 17-1303, Cybersecurity Workforce Improvement Program, the contractor shall comply with the Defense Acquisition Regulations (DFARS) 252.239.7001, Information Assurance Contractor Training and Certification, and all cybersecurity requirements stipulated in this task order. These requirements shall apply to all Contractor personnel performing one or more cybersecurity function identified in DoD 8570.01-M Information Assurance Workforce Improvement Program, regardless of contract labor category.

- The contractor shall ensure that all personnel accessing information systems have the proper and current information assurance certification to perform information assurance functions in accordance with DoD 8570.01-M. The contractor shall meet the applicable information assurance certification requirements including:
    - DoD-approved information assurance workforce certifications appropriate for each category and level listed in the current version of DoD 8570.01-M.
    - Appropriate operating system certification for information assurance technical positions as required by DoD 8570.01.
- The contractor shall provide the certificate issued by the certification authority for information assurance certification of personnel performing information assurance functions.

In accordance with AFMAN 17-1303, Contractor personnel shall meet the following additional requirements:

- Contractor personnel performing Cybersecurity functions for systems providing enterprise capabilities or services to Air Force end users worldwide shall attain and maintain, at a minimum, a level III baseline certification in the applicable Cybersecurity Workforce Category.
- Contractor personnel performing Cybersecurity functions for systems that are networked and interconnected, but do not provide enterprise capabilities or services to Air Force end users worldwide shall attain and maintain, at a minimum, a level II baseline certification in the applicable Cybersecurity Workforce Category.
- Software developer, engineer, and programmer positions requiring less than 4 years experience shall maintain an IA System Architect and Engineer (IASE) level I.
- Software developer, engineer, and programmer positions requiring more than 4 years experience shall maintain an IA System Architect and Engineer (IASE) level II.

5.5.2 Information System Security Officer

The contractor shall provide a dedicate Information System Security Officer (ISSO). The ISSO will work in conjunction with a multi-contractor team in support of Cybersecurity, FIAR IT, continuous monitoring, and other emerging compliance requirements.

5.5.3 Application Cybersecurity

Cybersecurity shall be integrated into the overarching Systems Engineering process as well as Cybersecurity events and activities included on the IMS. The Contractor shall identify, manage, verify, and implement Cybersecurity requirements and Cybersecurity controls, in the same manner as all other system requirements, ensuring traceability.

5.5.4 Information System Certification and Accreditation

The contractor shall work with other contractors, government personnel, and the Security Control Accessor Representative (SCAR) team to establish, and maintain AFM's security posture in accordance with applicable statutory, regulatory, and STIG guidance. The contractor shall:

- Support all efforts necessary to obtain and maintain AFM's Authorization to Operate (ATO).
- Develop any necessary artifacts and test plans required to obtain and maintain the ATO.
- Store and maintain artifacts in eMASS.
- Implement, test, and continuously monitor cybersecurity controls.
- Advise the AFM PMO on security compliance issues impacting system operations.
- Develop Plan of Action and Milestones (POA&M) to resolve, mitigate, and track vulnerabilities.

5.5.5 Interoperability Certification

The contractor shall obtain and maintain AFMs Joint Interoperability (IOP) Certification in accordance with DoDI 8330.01 Interoperability of Information Technology (IT), Including National Security Systems (NSS).

6 Service Delivery Summary

6.1 Service Delivery Summary

The following Service Delivery Summary (SDS) will guide overall performance of the Task Order (TO). The following criteria will be used to determine if performance requirements are met.

Performance Objective	Performance Threshold/Standard	Paragraph	Method/Frequency of Assessment and Inspection Procedure
System Administration	The system shall be available 99.7% of the time except for scheduled maintenance.	5.3.1	• Periodic Assessment • PM will review Monthly Status Report
Number of defects recorded during the first 90 days following a version release.	• No more than 5 defects identified during the first 90 days of any major release. • No more than 2 defects identified during the first 90 days of any major release. • No defects resulting from any patch.	4.1.8	• 100% Inspection • Review Defects reported in Serena Business Manager. • Review Quality Control Activities. • Review reports.
Number of software problem reports not corrected during GAT.	• There should be no severity I and II SPRs. For severity III-V SPRs the following applies: • No more than 5 SPRs for any major release. • No more than 2 SPRs resulting from any minor release. • No SPRs resulting from a patch.	4.1.8	• 100% Inspection • Review SPRs in Serena Business Manager. • Review Quality Control Activities. • Review other reports.
Delivery of deliverables identified in this PWS.	• 95 percent of all deliverables will be delivered on time, in the proper format, and error free. • Remaining 5 percent delivered no later than 5 days after the initial due date.	7.6	• 100% Inspection • Review of delivery to verify delivery and acceptance.
Help Desk Quality • Problem Reporting • Problem Correction • Timely Response	• No more than 2 reopened tickets per month. • Critical DR's fix or workaround provided within 48 hours with full resolution within 7 days. • Major DRs fix or workaround provided within 72 hours with full resolution within 45 days.	4.1.3	• 100% Inspection • Review DRs in Serena Business Manager. • Review Quality Control Activities. Review other reports.

7 Deliverables

7.1 Contractor Submission

Deliverables are to be transmitted with a cover letter, on the prime contractor's letterhead, describing the contents, electronically through GSA's web-based procurement system, ITSS, and to any other destination(s) as required per the Government's request. The contractor shall provide hard copy deliverables as required per the Government's request. All deliverables shall be produced using recommended software tools/versions as approved by the Government. All reports shall be accomplished utilizing the MS Office Software Suite to include MS Project as required.

7.2 Government Review

Government personnel will have 10 workdays to review deliverables (to include resubmissions) and provide written acceptance/rejection. Government representatives and/or the applicable Contracting Officer Representatives (CORs) will notify the contractor of deliverable acceptance or provide comments in writing. The contractor shall incorporate Government comments, or provide rationale for not doing so within 5 days of receipt of comments. Government acceptance of the final deliverable will be based on resolution of Government comments or acceptance of rationale for non-inclusion. Additional changes volunteered by the contractor will be considered a resubmission of the deliverable.

7.3 Deliverable Rights

All information such as software, data, designs, test materials, documents, documentation, notes, records, software tools acquired, and/or software source code and modifications produced by the contractor under this PWS shall become the sole property of the U.S. Government, which shall have unlimited rights to all materials and determine the scope of publication and distribution. The contractor shall be required to deliver electronic copies of all documents, notes, records and software to the Government upon termination of the task order or expiration of the task order. The Government shall retain ownership of all proprietary information and intellectual property generated under this task order.

7.4 Transfer of Ownership

All data and documentation, including all studies, reports, spreadsheets, software, data, designs, presentations, documentation, etc., produced by the contractor or for the Government using this PWS are the property of the Government upon its taking possession of task deliverables or upon termination of the ask order or expiration of the task order.

7.5 Monthly Invoice

The contractor shall provide a monthly invoice, no later than the 15th calendar day of the month following the monthly reporting period, to be submitted simultaneously with the MSR. Both documents shall be provided to applicable parties. The invoice shall include but not be limited to:

- Clear identification of all costs.
- Labor hours expended (for labor hours tasks) if applicable. The labor hours expenditure information shall include the identification of the employee name, labor category, hourly labor rate, and total number of labor hours expended.
- Timecards. The contractor shall provide a copy of each employee's timecard/sheet. The timesheet shall identify the contractor employee name and number of hours claimed per day.
- Travel costs.
- Supporting documentation for travel costs. Invoices including travel costs shall include supporting documentation as required by the Federal Travel Regulation (FTR) (receipts for all costs $75.00 or greater). Invoice submissions including travel costs shall include completed travel expense sheets (i.e. travel voucher) for each trip for each employee.

- The contractor shall comply with line item (i.e., per individual positions, different programs, program areas, etc.) billing requests.

7.6 CDRL Matrix

Sequence Number	Title	Paragraph	Frequency
A001	Contractor Quality Control Plan	3.1	30 days after contract start. Updated as necessary.
A002	Integrated Management Plan	4.1.1	30 days after contract start. Updated as necessary.
A003	Integrated Master Schedule	4.1.2	Monthly
A004	Program Performance Metrics	4.1.14	Monthly
A005	Monthly Status Report	4.1.15	Monthly
A006	Information System Contingency Plan	4.1.17	30 days after contract start. Updated as necessary.
A007	Incident Response Plan	4.1.18	30 days after contract start. Updated as necessary.
A008	Information System Security Plan	4.1.19	As required.
A009	Information Support Plan	4.1.20	As required.
A010	Department of Defense Architecture Framework Artifacts	4.1.21	As required.
A011	Interface Control Document	4.1.22	As required.
A012	Change Management Documents	4.1.3	30 days after contract start. Updated as necessary.
A013	Software Configuration Management Plan	4.1.13	30 days after contract start. Updated as necessary.
A014	Training Documents	4.1.23 5	As required.
A015	Technical Studies and Reports	4.1.24	As required.
A016	Software Development Plan	4.1.5	As required.

A017	Preliminary Design Document	4.1.6	As required.
A018	Software Design Document	4.1.7	As required.
A019	Software Test Plan	4.1.8	As required.
A020	Software Test Descriptions	4.1.9	As required.
A021	Software Test Reports	4.1.10	As required.
A022	Requirements Traceability Matrix	4.1.11	As required.
A023	Software Version Description	4.1.12	As required.
A024	System Administration Documents	5.3.1	As required.
A025	Data Base Administration Documents	5.3.2	As required.
A026	Hardware and Software Configuration Report	5.4.1	As required.
A027	Personnel Information Assurance Certifications	5.5.1	30 days after contract start. Updated as necessary.
A028	RMF Certification and Accreditation Artifacts	5.5.4	As needed.
A029	Interoperability Artifacts	5.5.5	As needed.

8 Personnel

8.1 General Requirements

All contractor employees shall meet the minimum general requirements listed below.

- All contractor personnel shall be capable of working independently.
- Strong written and oral communication skills in the English language. All contractor employees must be able to read, write, speak and understand English.
- Contractor personnel performing in a leadership capacity shall be capable of directing contractor personnel and interfacing with the Government and customers.
- Exceptional customer service skills.
- Strong time-management and prioritization skills.
- Ability to communicate applicable technical subject matter expertise to management and others.

8.2 Specific Expertise and Experience

The contractor shall provide personnel who are fully qualified to perform the requirements in the PWS. All contractor personnel must possess and apply comprehensive knowledge on multiple complex tasks and high impact assignments. Tasks require personnel to have the knowledge, skills, and abilities to determine innovative solutions to complex requirements. All personnel in information

technology positions must meet certification requirements identified in section 5.5.4 of this PWS. The team must have cumulative relevant experience in the following areas:

- Database Management
- Requirements Analysis
- Software Testing
- Software Development and Engineering
- Program Management Analysis
- Technical Report Design
- System Administration

8.3 Contract Management

The Contractor's Project Manager shall be the primary point of contact for the Government and shall be responsible for the management, content, and quality of work performed on this task order. The Contractor's Project Manager must be available to coordinate with Government representatives on a daily basis if required. The Contractor shall provide the Project Manager who is specified in their proposal for a minimum of the initial period of this Task Order, unless otherwise agreed between the parties. The Contractor shall provide a competent backup for the Project Manager in the event of a temporary absence and a competent replacement for the Project Manager in the event of the PM's extended absence (more than two weeks or other time as agreed between the parties).

The Project Manager must have credentials that substantiate that he or she has:

- Educational attainment that is appropriate for managing the type of work described in the PWS, both in size and scope.
- Mature experience in project management.
- Successful management of project tasks and coordination of employees in various labor categories and with various skills in projects of similar size and scope as the one identified in this PWS.
- Demonstrated experience managing, coordinating, and facilitating a team's efforts effectively and efficiently.
- Sufficient experience to be conversant in and have a working knowledge of each of the primary objectives of the PWS. The PM's experience must demonstrate that he or she can understand all aspects of the work, with the ability to direct the staff to perform successfully.
- Knowledge of Air Force management practices and program implementation.

8.4 Training

8.4.1 Contractor Staff Training

The Contractor shall provide fully trained, certified, and experienced staff for performance of this PWS Contractor personnel are required to possess the skills necessary to support the minimum requirements of the labor category under which they are performing. Training of contractor personnel shall be performed at the Contractor's expense, except when the Government changes the requirements during performance of an on-going task and it is determined to be in the best interest of the Government. This will be negotiated on a case-by-case basis. Training at Government expense will not be authorized for replacement personnel nor for the purpose of keeping Contractor personnel abreast of advances in the state-of-the-art, or for training Contractor employees on equipment, computer languages, and computer operating systems that are available in the commercial market.

8.4.2 Mandatory Government Training

Mandatory Government training shall be tracked and monitored. All required courses must be completed by the required dates by all contract employees. Mandatory government training classes may be completed during work hours. It is the intent of the USAF to provide 30 calendar days written notice of annual training requirements to the Contractor's Project Manager. The Project Manager will be responsible for notifying subordinate contractor employees. In the event the contractor does not

receive a 30 calendar day notice, the contractor is still required to complete the training by the specified required date(s).

8.5 Key Positions / Key Personnel

Key personnel are personnel proposed to perform in key positions. Key positions are those deemed essential for successful contractor accomplishment of the work to be performed. The contractor shall not divert key personnel to other projects or replace them without receiving prior authorization from the CO. All key positions require a bachelor's degree and 3-5 years of experience. A minimum of 5 years of specialized experience relevant to the key position is required to substitute work experience for education. The following positions will be considered to be key positions under this PWS:

8.5.1 Project Manager

The Project Manager shall be the primary point of contact for the Government and shall be responsible for the management, content, and quality of work performed on this task order. The Contractor's Project Manager must be available to coordinate with Government representatives on a daily basis if required. The Project Manager must have credentials that substantiate that he or she has:

- Mature experience in project management.
- Successful management of project tasks and coordination of employees in various labor categories and with various skills in projects of similar size and scope as the one identified in this PWS.
- Demonstrated experience managing, coordinating, and facilitating a team's efforts effectively and efficiently in a Time and Material/Labor Hour and Firm Fixed Price contracted environment within DoD.
- Sufficient experience to be conversant in and have a working knowledge of the tasks identified in sections 4 and 5 of this PWS. The PM's experience must demonstrate that he or she can understand all aspects of the work, with the ability to direct the staff to perform successfully.
- Knowledge of Air Force management practices and program implementation.

8.5.2 System Administrator

- The System Administrator (SA) must have the knowledge, skills, and abilities to complete all tasks identified in paragraph 5.3.1 of this PWS. The SA must have proven expertise in the following areas: Solaris 10 x86-64
- Symantec Netbackup 7.6
- Common Array Manager 6.9
- Oracle WebLogic Server 12.1.1.0
- Storage Area Network (SAN) and robotic tape library management
- Physical hardware installation, setup, troubleshooting, and decommission.

8.5.3 Database Administrator

The Database Administrator shall have the knowledge, skills, and abilities to complete all tasks identified in paragraph 5.3.2 of this PWS. The DBA must possess expert knowledge in administering an Oracle Database in a Solaris/Linux environment with expertise in the following areas:

- Procedural Language/Structured Query Language (PL-SQL) functions, packages, database views, constraints, and triggers.
- Oracle 11g Database Operations
- Oracle Development and Database Monitoring Tools like Oracle Enterprise Manager (OEM) and SQL Developer
- Veritas NetBackup
- Creating and Maintaining UNIX shell scripts
- Oracle Recovery Manager (RMAN)
- Source Code Control.

8.5.4 Lead Developer

The Lead developer shall have the knowledge, skills, and abilities to lead a development team and integrate multiple software configuration items into a cohesive end product. This individual must possess expert knowledge in the following areas:

- Hyper Text Markup Language (HTML).
- Java Server Pages (JSP).
- Java Script.
- J-Query and other Java Script Plug-Ins.
- Structured Query Language (SQL).
- Procedural Language/Structured Query Language (PL-SQL) functions, packages, database views, constraints, and triggers.
- Linux and Solaris Operating Systems.
- Oracle WebLogic.
- Database generated reports and files in Portable Document Format (PDF), Extensible Markup Language (XML), and Microsoft Products.
- Source Code Control.

8.5.5 Information System Security Officer

The Information System Security Officer (ISSO) shall have the knowledge, skills, and abilities to complete all tasks in section 5.5 of this PWS. The ISSO must have excellent verbal and written communication skills and be able to communicate with Cybersecurity practitioners as well as Financial Statement Auditors.

8.6 Personnel Retention and Recruitment

Government review and acceptance is required for all resumes of personnel proposed to support labor hour task orders and key personnel. The Contractor shall make every effort to retain personnel in order to ensure continuity until task order completion. If it should become necessary to substitute or replace personnel, the Contractor shall immediately notify the COR in writing of any potential vacancies and shall submit the resume(s) of replacement personnel within 14 calendar days of the notification. Additionally, for all new positions identified by the Government, the Contractor shall submit the resume(s) of proposed personnel within 14 calendar days of the Government's initial request. Upon Government acceptance of a personnel resume(s), the candidate shall be available to begin performance within 14 calendar days. The contractor shall ensure continuity of operations during periods of personnel turnover and long-term absences. Long-term absences are considered those longer than one week in duration.

9 Government Furnished Items

9.1 General

The Government shall provide, without cost, the facilities, equipment, materials and services listed below. The Government furnished property and services provided as part of this PWS shall be used only by the contractor only to perform under the terms of this PWS. No expectation of personal privacy or ownership using any Government electronic information or communication equipment shall be expected. All property at Government work sites, except for contractor personal items will be assumed to be government property unless an inventory of contractor property is submitted and approved by the CO/COR. Contractor personal items do not include computers, external drives, software, printers, and/or other office equipment (e.g., chairs, desks, file cabinets). The contractor shall maintain an accurate inventory of Government furnished property.

9.2 Property

9.2.1 Facilities

The Government will provide facilities at the authorized primary work location as specified in the PWS. Use of the facilities by contractor employees will include all utilities, telephone, janitorial services, and furniture for contractor employees performing tasks. The Government will provide the contractor access to buildings as required, subject to the contractor's employees obtaining the required clearances and approvals. The Government will provide up to a maximum of seven (7) workstations at the Government facility located at WPAFB, OH.

9.3 Equipment at Authorized On-Site Federal Work Locations

The Government will provide the following at authorized on-site Federal work locations:

- A suitable work environment (i.e., telephone, office space and furniture). Office space may include a private or shared cubicle, hoteling space (space reserved for temporary use), or other such space suitable for the work required.
- A personal desk top computer or laptop and auxiliary hardware and software.
- Network connectivity required to perform work assignments. Network and computer access rights commensurate with work assignments.
- The Government will replace items that are determined to be beyond economical repair by the COR unless damage or loss is determined to be due to contractor negligence.

9.3.1 Facilities and Equipment at Remote Work Locations

When work from a remote location is authorized by the COR, the contractor will not be reimbursed for costs associated with remote connectivity from cell phones, Wi-Fi access or Internet connection.

The contractor shall be responsible for ensuring the contractor employee has an adequate and safe office space that sufficiently protects Government equipment and information from loss, theft, or unauthorized access. The contractor's telework agreement, given a minimum of 24 hours of advanced notice, shall allow periodic inspections of the alternate work location can be undertaken. The purpose of the inspection is to ensure proper control and maintenance of Government-owned property and worksite conformance with safety standards and other specifications.

9.3.2 Materials

The Government shall furnish basic reference manuals, and any revisions, updates, and changes thereto for use by the contractor necessary to perform work assignments.

9.3.3 Validation of Government Furnished Items (GFI) and Equipment Inventory

The contractor shall develop and maintain a complete GFI inventory that shall be made available to the Government upon request. Within three (3) work days of receipt of any GFI, the contractor shall validate the accuracy of the materials and notify the COR, in writing, of any discrepancies.

NOTE: Validation shall consist of the Contractor checking for physical and logical completeness and accuracy. Physical completeness and accuracy shall be determined when all materials defined as Government furnished are provided. Logical completeness and accuracy shall be determined when all materials defined and associated with a program, system, or work package are provided.

9.4 Government Equipment and Contractor Facilities

The Government will provide equipment to the Contractor as GFE (Government Furnish Equipment) for use off-site if the Government is unable to provide sufficient on-site space and equipment to perform this requirement. Such GFE shall be housed and maintained at a Contractor facility located in the proximity of Wright Patterson AFB (within a 50 mile radius) unless an alternate location is approved by the Government. GFE will be turned over to the Contractor in conjunction with the Inbound Transition Joint Inventory described below. The Contractor shall be responsible for all GFE

in accordance with the provisions of the Government Property clause of this contract, which is hereby incorporated by reference if not otherwise included in the Contractor's basic Alliant GWAC.

9.4.1 Inbound Transition Inventory

The Contractor shall complete the Inbound transition Joint Inventory no later than thirty (30) days after contract start. The Contractor and a Government PMO Team member shall conduct a joint inventory of all GFP. The Government shall furnish a current inventory list against which the actual physical inventory will be verified. During the joint inventory, the Contractor and a Government PMO Team member shall jointly determine the working order and condition of all GFE. The Contractor shall document the condition of all equipment. The Contractor shall notify the Program Manager in writing within five (5) working days of completion of the joint inventory of all missing or unsuitable items for use GFE.

9.4.2 Outbound Transition Joint Inventory

The Contractor shall participate and complete the Outbound transition Joint Inventory no later than ten (10) working days prior to the end of the last performance period. The Contractor and a Government PMO Team member shall conduct a joint inventory of all Government property. During the joint inventory, the Contractor and a Government PMO Team member shall jointly determine the working order and condition of all property. The Contractor shall document the condition of all Government property and notify the Program Manager in writing within five (5) working days of completion of the joint inventory. The Contractor shall resolve any discrepancies between the joint inventory and official government records.

The Contractor shall perform a final inventory of documents and materials during the outbound transition. The outbound transition activities shall include, but not be limited to:

- Orderly compilation, labeling, and packaging of all work and documentation in progress.
- The provision of internal worksheets, aids, and other program developed and funded products that support the day-to-day management and customer support activities.
- Identification of upcoming scheduled user training, help desk support issues, risk items, open action items, hardware and software issues/concerns, and security issues/concerns.

9.4.3 Annual Inventory of GFE Lists

The Contractor's Equipment Inventory Manager Team shall perform an annual GFE Hardware/Software inventory, on or about the anniversary date of this task order, or at a time as otherwise agreed to by the Government. The results of the inventory shall be provided to the AFM system PMO.

9.4.4 GFE Inventory Management

The Contractor shall manage and update the inventory lists stipulated in this PWS on an on-going basis throughout the contract/task order period of performance.

9.5 Use of Government Property

9.5.1 Desk Telephones

Government telephones are provided for use in conducting official business. Contractor employees are permitted to make calls that are considered necessary and in the interest of the Government. The contractor shall follow the same policies as Government personnel for telephone usage.

9.5.2 Electronic Mail (E-mail)

All Government e-mail access and use by contractor employees shall be in support of the individual's official duties and task responsibilities. All information that is created, transmitted, received, obtained, or accessed in any way or captured electronically using Government e-mail systems is the property of the Government. Contractor employees shall have clear identification in their e-mail signature block

that identifies themselves as contractor employees. Contractor employees are prohibited from forwarding e-mail generated from a Government provided e-mail account to personal mobile devices.

9.5.3 Copiers

Copiers are to be used to copy material for official Government business only in the performance of the tasks in this PWS.

9.5.4 Fax Machines

Contractor employees shall not use fax machines for other than official Government business in the performance of the tasks in this PWS.

9.5.5 Computer and Internet

All Internet and electronic media access accomplished by contractor employees (utilizing Government furnished equipment) shall be for official Government business in the performance of the tasks in this PWS.

9.5.6 Canvassing, Soliciting, or Selling

Contractor employees shall not engage in private activities for personal gain or any other unauthorized purpose while on Government-owned or leased property, nor may Government time or equipment be utilized for these purposes.

9.5.7 Security Violations Using Government Equipment

Any contractor violating Government security policies, guidelines, procedures, or requirements while using Government equipment or while accessing the Government network may, without notice, have their computer and network access terminated, be escorted from their work location, and have their physical access to their work location removed at the discretion of the CO/COR. The CO/COR will notify the contractor of the security violation and request immediate removal of the contract employee.

10 Administrative Considerations

10.1 Personal Service

The client determined that use of the GSA requirements contract to satisfy this requirement is in the best interest of the Government, economic and other factors considered, and this PWS is not being used to procure personal services prohibited by the Federal Acquisition Regulation (FAR) Part 37.104 titled “Personal Services Contract”. The Contractor agrees that this is a non-personal services contract. The Contractor is not, nor shall it hold itself out, to be an agent or partner of, or joint venture with, the Government.

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

10.2 Privacy Act

Work under this PWS requires that personnel have access to Privacy Information. Contractor personnel shall adhere to the Privacy Act, Title 5 of the U.S. Code, Section 552a and applicable USDA rules and regulations.

10.3 Section 508

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