# Application Services –Small Business Companion

***Information System Support Services***

# Task Order Performance Work Statement (PWS)

|  |  |
| --- | --- |
| **Name:** | Mr. Gregory New |
| **Organization** | 448 SCMW/OMO-Hill |
| **Address:** | *6009 Wardleigh Rd, Bldg. 1209 Hill AFB, UT 84056* |

**Executive Summary**

Services are required for Material Support Division Information System (MSDIS) development/modernization (Dev/Mod), Low Demand/Low Density Requirements Management System (LD2RMS) and Information Technology (IT) related support.

# PURPOSE

The purpose of this task order is to support information system sustainment, Material Support Division Information System (MSDIS) development and sustainment, and information technology (IT) support. MSDIS has users across the Air Force Sustainment Center (AFSC), Major Commands and Defense Logistics Agency. IT services will directly support the 448 Supply Chain Management Wing-Hill, which includes Wing Staff offices and the 748 Supply Chain Management Group (SCMG) and 948 SCMG and the associated squadrons and staff offices.

Related to system development for MSDIS, the capability requirements are: Completion of the problems/requirements outlined in the Problem Statement (PS) approved by OSD for each development effort. The MSDIS PS approved for the FY16 Dev/Mod effort includes requirements in the Depot Supply Chain Management Analysis Tool, Spares Requirements Review Board, Metrics Financial Tool which includes the Capture project, Enterprise Materiel Solution modules of MSDIS. The government expects that these requirements will continue to be worked in FY22 and FY23 and will follow a similar level of effort. Additional MSDIS requirements are: Sustainment which includes resolution of bugs/issues identified by the user community. In addition, the system must be maintained to information assurance standards, to include, the DISA Security Technical Implementation Guide (DISA STIG), Biennial Notice and Consent Certification, Section 508 compliance and information assurance controls listed Enterprise Mission Assurance Support Services (eMass).

Related to system sustainment for MSDIS and Low Demand/Low Density Requirements Management System (LD2RMS) the capability requirements are research and resolve identified bugs/errors. Ensure system compliance with cybersecurity and information assurance mandates.

Related to IT support, the capability requirements are, Server administration (Cloud One- Microsoft Azure or Amazon Web services), Information Assurance duties, Cyber Liaison (CL) duties, (in processing and out-processing of personnel, provisioning, shared drive permissions etc.), Risk Management Framework (RMF-certification and accreditation) of organization defense business systems, Organization SharePoint administration, IT asset tracking and custodian duties.

# SCOPE

This effort will include system development and sustainment for MSDIS. MSDIS is a suite of seven modules that support logistics business processes designed to bridge a critical gap that exists between Commercial/ Government off-the-shelf (COTS/GOTS) applications (e.g., Microsoft Office Suite) which are not robust enough to handle complex office automation requirements and aged legacy systems (e.g., D200 Requirements Management System) too difficult and expensive to modify. MSDIS further replaces a variety of unique disparate tools and capabilities with robust web-based solution employed across the Enterprise supporting standardization and streamlining initiatives. MSDIS agile development principles meet the business office automation requirements that come from Continuous Process Improvement (CPI) initiatives and a changing operating environment. The modules are described below:

*Spares Requirement Review Board (SRRB):* The SRRB is a Program Objective Memorandum (POM) process for development of Cost Per Flying Hour (CPFH) spares factors across all Major Commands (MAJCOMs) initiating CRB (CRB) process. It is used to consolidate customer spare requirements. The SRRB module facilitates the early identification of forecast gaps between the financial and supply chain requirements. Air Force Life-Cycle Management Center (AFLCMC) weapon system managers distribute to all stakeholders the program changes using the template section of the system. Requirements comparison reports facilitate effective collaboration efforts of all stakeholders to meet Air Force (AF) strategic operation and budgetary objectives. Future enhancements will continue to improve the current process that has demonstrated an overall 18% reduction in forecast gaps valuing an average of $490M annually.

*Planning for Defense Logistics Agency (DLA) Managed Consumables (PDMC):* The PDMC capability in MSDIS is the AF Enterprise solution for forecasting deviations in historical demand trends and submitting Demand Data Exchanges (DDEs) to DLA to override baseline requirements with program changes. The current capability integrates data from multiple core command AF systems to calculate the End Item (EI) requirements forecast. The EI forecast is then matched to its unique Bill of Material (BOM) to determine the baseline DLA spares requirement. Process initiators across the Air Force use the PDMC capability to build Demand Input Templates (DITs) based on established demand triggers to communicate new or changing requirements that deviate from historical demand trends to DLA planners.

*Depot Supply Chain Management Analysis Tool (DSCM AT):* The DSCM AT module provides depot maintenance parts supportability analysis and is critical to weapon system availability. The capability successfully brings all maintenance and supply stakeholders (AF and DLA) into a single supportability information system and builds cohesion and cooperation in strategically solving parts support problems. DSCM AT provides analysis of anticipated requirements over an eight-quarter rolling future horizon, against available and anticipated resources across all AFMC/AFSC Air Logistic Complexes (ALCs). It also provides a rolling twelve-month historical view to assess performance to date. DSCM AT is the automated solution that brings stakeholders together to agree on a common plan for an end item and to collaborate on how to support the end item. It serves as the solution for accountability and execution for all supply chain stakeholders.

*Enterprise Material Support (EMS):* MSDIS also contains a module that is utilized across the Air Force Supply Chain Enterprise to work various data calls, standardize and streamline business processes, and properly account for critical Air Force resources. Specific functionality supports:

* + Budget variance narrative reporting
  + Spares termination tracking
  + Congressional inventory accounting (DD-1000)
  + Homeless item tracking
  + Inter-service support program reporting
  + Spares computation collaboration and signature collection process
  + Workload assignment and tracking for Purchase Requests (PRs), Military Interdepartmental Purchase Requests (MIPRs), and materiel screening documents/processes
  + Material loan tracking
  + Suspended asset management and tracking
  + Depot organic repair workload collaboration
  + Deferred disposal code tracking

*Metric Financial Tool (MFT)*: MFT is used by financial analysts, managers and commanders across the 448 Supply Chain Management Wing (SCMW) and beyond. MFT provides tracking of all requirements, budgets, funding received and distributed, forecasts and complete program execution in a user-friendly dashboard environment consistent with Art of the Possible initiatives. The system also generates metrics and facilitates unfunded/unbudgeted requirements and coordination, and stoplight/forecast narrative collection and collaboration. The existing business need is to manage financial execution across a $5 billion materiel sustainment enterprise. The objectives enabled by this system include validating compliance with public law (propriety of funding/purpose/time/amount), managing materiel executions, managing overhead execution, managing compliance with targets and forecasts, collaborating and correcting discrepancies, and insuring 100% execution of available funding on valid requirements. This effort represents the critical functions of senior leadership, supply chain and other stakeholders (PZA/DCMA) across the enterprise and must be managed and developed on an ongoing basis, to the extent that funding is made available for materiel sustainment operations. MFT requires execution and tracking capability, also known as capture, which requires dynamic programming of several high priority Change Requests (CR) to improve functionality for the enterprise.

Awarded vendor will support the development of the Art of the Possible requirement to enhance enterprise-wide. Standardize the MFT tool to provide a single IT solution to view the acquisition process from requirement identification, sourcing approach, through Purchase Instrument generation, contract award, management and close-out; tracking of all Consolidated Sustainment Activity Group (CSAG) funds through effort. Vendor will automate and ease the use for standard metrics and workload reporting and tracking of CSAG funds and requirements at the NIIN level for the enterprise. Completing concurrent CR programming efforts in a timely manner; that may contain extensive programming requires and system interfaces within the CRs. Expanding current MFT requirement capabilities and enhancing the efforts to track Financial Improvement and Audit Readiness (FIAR), to including payment tracking from various systems and sources for CSAG funds. Programming efforts to allow for customizable charts to

support current approved monthly financial execution briefing format. Complete all approved and future requirements and CRs supporting requirements capability to track associated purchase instruments through the acquisition and execution process of contract award, execution, delivery and closeout.

*Management Analysis Tool (MAT)*: MAT is used by resource and performance managers, resource advisors and supervisors across AFSC and beyond. The system is designed to facilitate organizational collaboration, routing and tracking of personnel actions, requests for travel, requests for premium time, requests for leave, extensive award allocations and distributions, validate system data, and automate and provide visibility for a series of labor- intensive management tasks consistent with Art of the Possible initiatives. The system generates mismatch reports and programmatically creates various personnel charts and tables. This system automated critical functions required to manage civilian personnel. The system provides leadership at all levels oversight and the ability to route, track and document all requirements associated with various personnel actions. These business processes will be required as long as civilian personnel management remains a part of Department of Defense (DoD) operations.

*Maintenance Engineering Project Sustainment Tool (MPST):* MPST is used by engineering stakeholders across the Air Force Supply Chain and beyond to approve, validate, prioritize, collaborate on, and document the requirements and execution of multi-billion-dollar CSAG-S engineering and Test Program Set (TPS) projects. The supported business processes include the management of sustaining engineering for CSAG-S managed assets. This function supports the improvement in reliability and maintainability of Working Capital Fund (WCF) managed components and will remain an ongoing effort for the life of material sustainment operations.

In addition, this effort will sustain LD2RMS. Currently, the tools are under DBShell, Daily Backorder Narrative (DBN) and Doc Log. However, these tools they are going through the registration process and will be re-named prior to contract award. These tools support supply chain management squadrons within the 448 SCMW.

The Low Demand Low Density Requirements Management System (LD2RMS) application contains unique management reporting capabilities specifically geared toward supporting Low Demand/Low Density (LDLD) Supply Chain Management (SCM) organizations. Internal to the (LD2RMS) system, there are 10 applications that are used to manage LDLD SCM. These applications consist of the Integrated Product Team (IPT) Database, Tobyhanna Army Depot (TYAD) Scheduling Tool, Requirements Authorization Worksheet (RAW), Form 800, Material Support Division (MSD) Repair Input, MSD Buy Input,

Depot Maintenance Interservice Agreement (DMISA) Tobyhanna Army Depot Data, Budget Execution Progress Report (BEPR), Document Backorder Narrative (DBN), and Document Log (Doc Log).

* + The IPT Database application is a forecasting tool which allows a Logistics Management Specialist (LMS) to manage D200A repair requirements at the IPT level. The application allows the LMS to manage the detailed planning of requirements execution by

NSN, Source of Repair (SOR), including time-phased schedules by month, and to maintain and adjust this plan throughout the fiscal year.

* + The TYAD Scheduling Tool application is a forecasting tool creating an 8-quarter delivery schedule with the current year in monthly buckets. Its purpose is to allow the LMS and Production Management Specialist (PMS) to manage the complex scheduling and monitoring of repairs at TYAD, the primary repair sources of the 415 SCMS. The current DMISA agreement calls for an 8-quarter delivery schedule to be prepared at

least annually and negotiated with TYAD to provide visibility for long-term resource and capacity planning and to facilitate pricing negotiations. The TYAD Scheduling Tool is used to develop, maintain, and house official delivery schedules for any work being accomplished at TYAD.

* + The Requirements Authorization Worksheet application is a purchase instrument

planning tool the helps facilitate requirement execution at the IPT level. Its purpose is to ensure funds are used for justifiable expenses backed by legitimate D200A requirements.

* + The Form 800 application is used to justify additional D200A requirements when the IPT needs to execute beyond the March actual year computation cycle to support the warfighter. The purpose is to ensure funds are used only for justifiable D200A requirements, and to ensure that all actions have been executed to generate such requirements in the next computation cycle.
  + The MSD Repair Input application is a form used to gather data about each repair purchase instrument. Its purpose is to gather purchase instrument financial and requirements data used in a variety of reports used by management and individual IPTs.
  + The MSD Buy Input application is a form used to gather data about each repair purchase instrument. Its purpose is to gather purchase instrument financial and requirements data used in a variety of reports used by management and individual IPTs.
  + The DMISA TYAD application is used to track and analyze the funding and production completions of TYAD workload in accordance with TYAD accounting, including the work breakdown structure, unit prices, line item inductions, and repair completions.
  + The Budget Execution Progress Report application is a weekly summary report for all levels of management as well as LMSs showing status of requirements and budget execution at the squadron, flight, unit, and IPT level. The report displays computed vs required buy and repair requirements, purchase requests processing data, and overall budget execution compared to target execution rates. The purpose of this report is to inform IPTs and management of the status of budget and requirement execution.
  + The Doc Log application provides item managers (IMs) an automated system/data base that assigns off line shipping documents. Prior to Doc Log, IM managers required to hand scribe off-line shipping documents in a dedicated book. Doc Log automates this process by IM inputting required information and producing a unique document

number.

* + The Document Backorder Narratives (DBN) application tracks the daily status of budget code “8” backorders and Mission Impaired Capability Awaiting Parts (MICAPs) at document level. DBN provides integrated product teams daily status of budget code “8” backorders and MICAPs at the document level, and allows the management of scheduled completion dates, source of repair by month, and to maintain this plan throughout the fiscal year.

The remaining portion of this effort will be in support of IT related duties such as but not limited to, server and database administration (Cloud hosted Microsoft or Amazon Web Services), Information Assurance, Equipment Custodian, in processing/ out-processing of personnel,

Electronic Records management, Five Video Teleconference sites, Cyber Laison (CL) support for approximately 1,000 employees located at Hill AFB, a third information system (TeamCenter) may come online FY23 or 24.

1. **REQUIREMENT(S)/DESCRIPTION OF SERVICE(S)**
   1. **Systems Sustainment**

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

The contractor shall maintain the current baseline of the system and provide software change and problem fixes to these baselines as required. The contractor shall resolve government identified bugs/fixes. The contractor shall design, develop the resolution to the identified problem, test and package systems and software changes for the MSDIS and LD2RMS. The contractor shall provide to the Government all developed, modified, or converted source modules, processes, programs, scripts, operating instructions, databases, system files, documentation, test files and test conditions used to develop each approved system change request. All code-related sustainment actions shall be approved on Change Requests (CRs) through the AFMC Requirements Management Process. Specific tasks may include the following:

* + - Maintain existing systems and environments IAW disciplined engineering practices and sustain applications, databases and interfaces in compliance with applicable AF/DoD standards.
    - Support system sustainment activities to include maintaining existing legacy systems and environments and to sustain applications, databases and interfaces.
    - Research and resolve system driven error messages
    - Provide application services to support, maintain and operate systems or services, including resolving customer identified bugs
    - Complete monthly security testing and resolve the issues in accordance with AF

and DoD driven policy. The contractor shall have knowledge of security requirements and implement them throughout the system.

* + - If required, complete the re-coding tools from Classic ASP code language to .NET code language
    - The contractor shall be responsible for updating current user guides using Microsoft Office based on new functionality and establishing new user guides if one is not currently available. The updates shall be approved by the government functional advocate or program manager to ensure that it is accurate.
    - Pull data queries based on customer request to support system business process

The contractor shall assist with testing, implementation and transition of reports functionality to an AF approved system to support overall AF IT initiatives (ESCAPE, LIMS-EV etc).

# MAT Module Sustainment

* + - * Support system sustainment activities to include updating all existing capabilities for personnel actions, TDY requests, OT/CT requests, leave requests, appraisal awards.
      * Provide support for all current and future approved capability updates to include overhire approval process, personnel action metrics and dashboard, adding additional personnel action types, modifying request or selection details for personnel actions, civilian execution plan, status of discipline, coordination of telework, award and other packages, asset traceability, in/out processing checklists, etc.
      * The contractor shall be responsible for providing module support on a daily basis to review actions and adjust logic, coordination, routing, and update action statuses

# MFT Module Sustainment

* + - * Support system sustainment activities to include updating all existing capabilities for current/end of month status of funds, stoplight metrics, distribution and forecasting of funding, financial metrics and reporting, coordination and tracking unfunded requirements, requirements capability tracking for purchase instruments from requirement identification through contract award and closeout
      * Provide support for all current and future approved capability updates to include updating all current capabilities from .asp to .net framework. Updating all requirements and reporting to utilize new crosswalks for .net. Allow for customizable charts to support current approved monthly financial execution briefing format. Complete all approved and future requirements supporting requirements capability (also known as CAPTuRE) to develop requirements and track associated purchase instruments through the acquisition and execution process of contract award, execution, delivery and closeout.
      * The contractor shall be responsible for providing module support on a daily basis to review actions and adjust logic, coordination, routing, and update requirement statuses

# Enterprise Materiel Support (EMS)

The EMS module is comprised of multiple business automation tools. The contractor shall maintain the current software baseline and work through other tasks as identified:

* + - * Budget Variance Narrative Report (BVNR). The contractor shall add functionality to allow grouping by weapon system and reproducing narratives to be applied across multiple NSNs. The contractor shall add functionality to allow other complexes (Warner Robins and Oklahoma City) to use the tool. The contractor shall add functionality to help produce budget brochures.
      * Computation Signature Sheets (CSS). The contractor shall modify the tool to accept files from ESCAPE as necessary. When computation signatures are automated in ESCAPE, the contractor will decommission the CSS functionality in EMS.
      * DD-1000. The contractor shall remove IMS and PMS codes and replace them with the planner code.
      * Deferred Disposal Code Tool (DDCT). The contractor shall modify the tool to accept files from ESCAPE as necessary. When deferred disposal management is automated in ESCAPE, the contractor will decommission the DDCT functionality in EMS.
      * Inter-service Support Program (ISSP). The contractor shall add functionality to allow users to duplicate and copy existing records to help streamline the creation of new records. Further, the contractor shall add drop down functionality for “contact” and “from” to eliminate errors from manual entry. The contractor shall modify metric reports to include records entered on the 31st of the month.
      * Loans. The contractor shall expand the tool for managing assets loaned from Oklahoma City and Warner Robins ALCs. The contractor shall help provide training as needed to the new locations.
      * Workload Assignment and Tracking Tool (WATT) – Military Interdepartmental Purchase Request (MIPR). The contractor shall add an action log to track users that made different inputs. The contractor shall add fields for better tracking (e.g., processing system, FMS, service fees, temporary number, and pending block).
      * WATT – Purchase Request (PR). The contractor shall add an action log to track users that made different inputs.
      * WATT – Screening. The contractor shall add an action log to track users that made different inputs.
      * Suspended Asset Tool (SAT). The contractor shall continue to expand SAT to include stock readiness assets. The contractor shall generate reports to streamline metrics reporting for suspended and stock readiness assets.
      * Workload Collaboration Tool (WCT). The contractor shall participate in hot wash events after each cycle and help develop tool enhancements to address issues identified. The contractor shall make data load changes to accommodate D200A being subsumed by ESCAPE.
      * Terminations Tracking. The contractor shall modify the tool to accept files from ESCAPE as necessary. When terminations tracking is automated in ESCAPE, the contractor will decommission the terms tracking functionality in EMS. The contractor shall add source of supply details to the all NIINs in termination.
      * Homeless NSNs. The contractor shall decommission the Homeless NSN tool as it is no longer required.

# Systems Development, Migration and Integration

Contractor will complete Development/Modernization (Dev/Mod) requirements that have been documented and approved through the AF driven Service Development and Delivery Process (SDDP) and Problem Statement (PS) Process for MSDIS. Individual requirements that

are approved by the overarching processes (SDDP and PS) will then be approved separately by individual requirement on CR through the AFMC Requirements Management

Process. Approved CRs will be entered into a ticketing system (supported by this contract) and prioritized by the government. Systems development, migration and integration requirements must comply with applicable documents and standards specified in Section 8 of this TO PWS.

* + - Conduct software development to include increased programming efforts of modules, timely review and completion of CRs and newly identified efforts, software security, web services development, web services testing or other IT device applications and testing, security layer integration, database clean-up, data wrapping and data conversion.
    - Adapt programming language from .asp to .net, where needed.
    - Vendor will coordinate with government to secure Interface Control Documents (ICD), identify if source data is already being obtained by MSDIS, or if new source data is required, a CR and ICD will be obtained by the vendor.
    - The contractor shall be responsible for providing module support on a daily basis to review actions and adjust logic, coordination, routing, and update requirement statuses.
    - Vendor will be required to work multiple CRs concurrently to deploy functionality within a timely manner.
    - Develop schedules and implementation plans, including parallel operations, identification of technical approaches.
    - Perform system performance tuning, system re-hosting and integration services.
    - Utilize Government-Off-The-Shelf (GOTS) or approved Commercial-Off-The-Shelf (COTS) tools for systems design and development.
    - If applicable, ensure compliance with the USAF Implementation Baseline (IB). The IB is applicable to IT programs, new systems/applications, major increments and/or applications migrating to new infrastructure environments as identified in the baseline documentation.

The contractor shall be responsible for following applicable Configuration Management policies including source code management. The contractor shall provide business process improvement support that includes all activities involved in helping improve customer data systems through business process redesign, including rethinking program design, and aligning information technology infrastructures with business missions, goals, and objectives. The contractor shall maintain, in a current status data dictionary, any subsequent code changes, additions that are developed after the source code(s) are established; documentation developed under this and its predecessor task orders. The contractor shall provide solutions that meet

confidentiality, data integrity, authentication, and non‐repudiation requirements. The

contractor shall follow applicable AF guidance regarding PKI and authentication standards. The contractor shall primarily be responsible for integration of schedules between Programmers at Hill, communication of requirements/initiatives that may have an impact on the contract/contractor/system and may attend the Configuration Control Board etc. in support of these additional requirements. The contractor shall be responsible for documenting system data usage through interface control documents and researching AF data warehouses to determine if data requested by the government is available. The contractor shall review government provided detailed requirements documents and provide comments and areas of required clarification. The contractor shall perform system development and security testing prior to release of code and facilitate customer acceptance testing.

# 3.3. Information Services

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

The contractor shall provide application and content presentation services that identify and exploit existing services, create new Service-Oriented Architecture applications and

data services, create presentation services, define, align and register vocabularies, expose information assets for discovery in the Metadata Environment (MDE) for Communities of Interest (COI), provide wrapping services and provide data layer connectivity.

# Web Services

Create and maintain web services using standards as defined within the Enterprise Architecture to enable sharing of data across different applications in an enterprise. In addition, contractor shall provide SharePoint support for 448 SCMW-Hill level site, 748 SCMG News and Information SharePoint site, assist with suspenses, answer questions and provide basic training to government appointed SharePoint site owners.

# Service Lifecycle Management

Generate necessary design and implementation artifacts that will support life-cycle management, defined as service development, testing, certification, registration, sustainment and evolution aligned with defined requirements. The design and implementation artifacts are owned by the Government and provided to the Government representative prior to the end of the task order at no additional cost to the Government.

# Data Stores

The contractor shall be responsible for maintaining data required in information systems. Data is received through manual and automated methods. This includes:

* + - * Create and maintain data stores.
      * Provide services such as data cleansing, redundancy resolution, and business rule validation
      * Monitor and maintain these data stores to ensure data availability, accuracy, precision and responsiveness.
      * Upload data files that are received through manual methods (SharePoint, CD etc.)
      * Work with Q310 database, Self Service Data Access Request (SSDAR) and Global Combat Support System (GCSS) AF Data Services or other authoritative source system database to report, research and resolve issues with data tables and elements if they arise.
      * Monitor queries to ensure the correct data is being pulled
      * Investigate/research potential source data systems

# Systems Operations

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

The contractor shall provide operational support services including, database administration, systems administration, customer training and help desk support of both legacy and new applications and systems in accordance with AFI 17-100 Network Operations and

DoD 8570.01M Information Assurance Workforce Improvement Program and in compliance with the target enterprise architecture.

# Database Administration

The contractor shall provide database administration support for logical and physical designs for information systems (currently MSDIS and LD2RMS) managed or hosted by the organization.

The contractor shall accomplish the following data services: create and test backups, cleansing services, integrity verification, and implement/manage access controls, while ensuring maximum availability and performance for an NIST SP 800-53 Revision 4 system. The contractor shall assist developers of data exposure services on efficient and effective use of the database.

This includes: performance monitoring, research and resolution of identified issues, not limited to but represented by issues associated with index corruption and other database errors.

The contractor shall provide real-time diagnostics on database and server performance to deliver the ability for improvement and or reduce degradation in performance. The contractor shall work with software developers (3.1 and 3.2) to resolve database performance issues.

The contractor will provide SQL (Structured Query Language) Report Services reports as needed and approved by the configuration control board (CCB). Reports will be protected by security groups designated by the CCB. Modification and removal of reports will also be approved by the CCB.

The contractor shall support LD2RMS databases using best industry practices for necessary and emerging requirements such as, but not limited to, exporting SQL databases to other servers, developing, modifying and amending query tables, forms, queries and reports, adding new data associated with transitioning functionality to the new fiscal year, reviewing sample data, and verifying functions are working correctly. The contractor shall provide technical support and expertise for security and technical refreshes. Functionality under this paragraph includes LD2RMS.

The contractor is required to be in compliance with the USAF Cloud initiative. When directed the LD2RMS system will be migrated into the authorized USAF Cloud. The contractor is required to engage with the cloud solution team to provide necessary migration support. Upon successful migration, the contractor is required to support various IaaS (Infrastructure as a Service) and PaaS (Platform as a Service) architectures implemented by the cloud migration support team.

This will include the associated support and maintenance of the database, application services, virtual machines, web functions, cloud storage, virtual routing, and cloud security applications. The contractor is required to modify or update code for the LD2RMS application to support any cloud authentication and security requirements. The contractor is required to perform all necessary STIG (Security Technical Implementation Guides) management and patching within the cloud environment.

# Systems Administration

This level of effort is based on organization owned systems and hardware and will be reduced as systems are re-hosted IAW Federal Data Center Consolidation Initiative. The contractor shall ensure smooth continuation of operation; manage and control security to the system; determine which users will have access to the various applications and, which forms, functions and reports a user can access; set‐up new users and provide access to only those forms, functions and reports required for the performance of the individuals’ duties; perform audits of user activity monitoring system usage; perform all auditing functions within established security guidelines; and respond to the Information Assurance Manager direction and ensure system security is maintained.

The contractor shall provide System Administration for the servers assigned (will be part

of USAF CloudOne) and data base system; allocate, manage and monitor space and storage requirements for the database; monitor scripts utilizing the Database Consistency Checker (DBCC); review and check for file/table fragmentation and accomplishes appropriate action to de‐fragment database; maintain and monitor scheduled backups and ensure they are accomplished and verified to ensure restoration procedures are successful; and install software upgrades and track system licenses including software maintenance.

The contractor shall be responsible to provide administrative services to include individual and group access to applications, domains and systems through user registration and profile management; server configuration, disk space and directory management; resource management; and establishing and managing directory services.

The contractor shall provide individual and group access to applications, and systems through user registration and profile management; server configuration, disk space and directory management; shared resource management; and establishing and managing directory services. The contractor shall oversee the creation of user accounts in accordance with Air

Force policy and guidance, specifying the user’s identification data, group

memberships, security‐policy information and defining the user’s rights on the system. The contractor shall create and maintain volumes and directory structures; assign account, workgroup and print managers; administer directory distribution and replication; define and manage resources, and server passwords; support standard security mechanisms and trusted third‐party security servers; and synchronize security structures across servers.

If required, the contractor shall, in accordance with Air Force policy and guidance, configure, set up servers with both operating system and network operating systems software; acquire and upgrade hardware and software and associated addresses; develop installation documentation

and server images. The contractor shall follow Air Force configuration management policies. Create and maintain technical documentation. Configure the operating system and network operating system; include protocol details, user and group definitions, address

schemes, backup and restore processes, disk space mappings. Monitor and report on service level delivery, hardware configurations and access rights. Manage Windows Server domains and Active Directory, IP addresses, and firewall parameters. The contractor shall monitor, report, and analyze server performance statistics, install management agents and tune servers. The contractor shall remedy problems expeditiously using escalation and alert processes; also maintain a log of all activity for fault management.

The contractor shall develop server capacity plans, monitor current server workloads and project future workloads. The contractor shall provide problem diagnosis and resolution. The contractor shall perform hardware maintenance and repair in accordance with manufacturer warranty. The contractor shall perform change management to support changes in hardware configuration and workload/capacity changes.

The contractor shall mitigate vulnerabilities reported by security scans and industry reports, continually assess requirements, evaluate risks, and implement procedures to log, alarm and report security violations to the Information Systems Security Manager (ISSM) and Information System Owner (ISO). Ensure anti‐virus software agents and definitions are current on all servers. The contractor shall monitor events related to system security to identify any security breaches and to determine the extent and location of any damage; perform corrective actions to repair systems and notify the proper authorities if warranted. The contractor shall implement all TCNO’s and TCTO’s within the specified timeframes.

The contractor shall provide patch management. Patches that cannot be automatically applied will be manually implemented. The contractor shall perform automated server monitoring which includes network connectivity, CPU, memory, disk space thresholds, uptime, response time, and web server availability, and shall provide monthly reporting of these statistics and others which can be monitored using Air Force‐furnished utilities. Maintain and review server logs using Air Force‐provided log consolidation tools; log warnings and alerts should be reviewed daily in a proactive manner. The contractor shall maintain server inventory and

provisioning documents. The contractor shall maintain software inventory, warranty information, licensing and vendor contact information. The contractor shall notify the Air Force in the event of expiring support of hardware and software. The contractor shall maintain a clean server and surrounding area environment.

The contractor shall maintain currency of existing service offerings through research, development, deployment, and training. The contractor shall collaborate with software and hardware vendors on various projects and opportunities of interest to the Air Force (beta testing, training, certification programs, etc.) The contract shall develop and track progress toward long- and short-term goals. The contractor shall research and recommend enhancement products for purchase.

# GovCloud

* + - * + Contractor shall be responsible for all design and engineering associated with the Dev and MSDIS GovCloud platforms within the scope or responsibility boundaries defined by the AF for ordinary upgrades, necessary solution extensions, or enhancements.
        + Contractor shall maintain and document all AF-managed GovCloud configurations/environments associated with the MSDIS Dev/Prod and MSDIS solution. This shall follow a defined process and will be integrated with the larger MSDIS Configuration Change Board (CCB) or other such configuration control process.
        + Contractor shall hold regular periodic information system design reviews to ensure compliance standards are maintained and to track/manage platform configuration.
        + The Contractor shall manage all production issues associated with the platform and track identified findings to resolution in the AF designated system or software. The Contractor shall develop Plan of Action and Milestones to track work towards a finding to completion and file that information with system security control documents. The management of platform issues/helpdesk tickets will be integrated within the context of holistic MSDIS problem management.
        + Contractor shall document platform-related system and network security in Government directed documents to include, system security plan, Information Support Plan, Cybersecurity Strategy and changes to the system with regards to security and develop plan of action and milestones for fixes that are in work.
        + Contractor shall document and support a development lab (dev lab) certification and Authority to Operate (ATO) accreditation or other acceptable solutions in CloudOne or other AF designated hosting environment in the event that an alternative contracted solution similar to Hanscom milCloud (HmC) is unavailable.
        + Contractor shall provide diagnostics on the MSDIS database, server, services, or network performance to identify and correct solution degradation in performance.
        + Contractor shall resolve Government identified bugs/discrepancies associated with issues on any MSDIS and Dev GovCloud platforms or configurations Discrepancy Reports (DRs).
        + Contractor shall configure a scalable storage system/environment process that provides at least ten (10) years of record retention. Contractor shall recommend and configure for cost effective data retrieval and archiving functions to included current operational data, warm store, and archive storage processes (cold storage) or other technically feasible and economically viable recommendation.
        + Contractor shall extend the current MSDIS platform to include a fully configured Microsoft Azure compatible business analytic capability like Power BI or Tableau via Platform as a Service (PAAS, LAAS) to draw data from MSDIS and other sources to present to users and leadership in the form of analytic tools, metrics, dashboards, and reports.
        + Contractor shall extend the current MSDIS platform to include a fully configured Microsoft Azure compatible business process or workflow capability similar to Appian, Pega, or any comparable COTS solution.

The Data Management workstream combines a large set of related tasks which have already been underway for some time on the MSDIS program. The role for this workstream and several

others listed in the PWS represents a combination of system design, development, integration, and sustainment oversight. The tasks and activities associated with MSDIS Data Management will include the following requirements and activities:

* + - * + Contractor shall design and maintain the MSDIS platform solution data architecture, including: Data Ingestion, Curation, Analysis, and complex data preparation with Extract, Transform, and Load (ETL) or other data related services utilized.
        + Contractor shall create and maintain a Data Interface Strategy for MSDIS. The TSP will facilitate all aspects of Data Interface management to include authoritative source system recommendations, interface design, implementation, and compliance related Corporate Data Repository System (CDRS), Memorandum of Agreement (MOA), and/or Information Systems Management Tool (ISMT) support.
        + Contractor shall deliver current Work in Progress (WIP) and maintain a MSDIS Business Glossary.
        + Contractor shall deliver current WIP and manage all appropriate data models associated with the MSDIS platform including a Canonical model.
        + Contractor shall provide database administration support for all physical database schemas associated with MSDIS. Contractor shall provide system administration for all business intelligence capability resident on the MSDIS platform.
        + Contractor shall design, develop, and deliver MSDIS configuration(s) to support raw data file ingestion, data preparation, computations, business rule processing, and analytics to minimize processing time and maximize AF readiness. The ingestion zone should be compatible with current and future Cloud One or other AF designated hosting platforms ports and protocols.
        + Contractor shall create and test backups of data, provide data cleansing services, verify data integrity, implement access controls to the data, ensuring maximum availability and performance.
        + Contractor shall assist developers of data exposure services to efficiently and effectively use the database. This includes performance monitoring and research and resolution of any identified issues, including index, corruption and other database errors.
        + Contractor shall develop Structured Query Language (SQL) code/operations for any business rules or transformational actions required in support of MSDIS.
        + Contractor shall configure deliverable(s) to provide blended flat file outputs from MSDIS and other data elements to fulfill AF outbound and downstream data requirements.
        + Contractor shall resolve Government identified bugs/discrepancies associated with issues in any data solution elements leading to DRs.
        + Contractor shall develop ETL or other programming logic as needed to provide containerized outputs (currently flat files) for consumption by PTC/SPM or any other trading partners.
        + Contractor shall configure a Microsoft Azure data lake (blob storage) with an associated file directory and move scripts structure to enable data staging.
        + Contractor shall maintain the current MSDIS baseline and provide software changes and problem/bug fixes to these baselines as required.
        + Contractor shall interrogate, map, and document source to target schema and data relationships. This action may include discovery and documentation of production data in text/filler fields and conversion to appropriate target source file formats.
        + Contractor shall identify, refine, and maintain a data mapping of input system sources, MSDIS use, and outputs consistent with mnemonics recorded in CDRS.
        + Contractor shall document business rules, processing logic, and transformational actions by system.
        + Contractor shall deliver compliant future state interface(s) with several legacy and emerging application(s) or system(s) to ingest demand signals and other relevant data against MSDIS’s existing production cloud and database structures and make ready for downstream systems. Interfaces will be based on identified need through the capability onboarding process, new business processes or leadership request (estimate 15-25 interfaces per year) and prioritized if needed.
        + Contractor shall continue to support all existing heritage/legacy interfaces currently in MSDIS.
        + Contractor shall design, develop, and deliver data interface and cloud to cloud (C2C) transfer configurations utilizing port 443 (or other future port options) and Akamai Global Content Delivery System (GCDS) (or other future software/hardware) to include the following solution patterns:

Manual Uploads

Secure File Gateway (SFG)

Representational State Transfer Application Program Interface (RestAPI)

DLA Defense Automatic Addressing System DAAS Global Data Exchange (GEX)

AFLCMC/HNII’s Enterprise Application Integration (EAI) (replacing Enterprise Service Bus (ESB) and ESB Message Mediator (MM))) or other designated induction and C2C connection hardware/software

Other induction methods as they emerge from AF or Cloud One platforms

# Customer Training

The contractor shall support training on new functionality and to new users on MSDIS. All training will be completed in conjunction with government functional advocate support. Travel may be required in support of this requirement. The training will include the following tasks:

* Provide on-site training at Government locations and training via audio-visual conferencing service
* Develop, maintain and/or update student and instructor training programs and materials.
* Provide a written test case for new functionality that may also serve as a written training tool
* Ensure training stays current with the services offered throughout the life of the Task Order
* Establish user guide for MSDIS modules.
  + Update current established user guides in Microsoft Word format annually based on new development or updates to existing functionality. Work with government functional advocates to ensure updates are accurate.

# System Service Desk Support

The contractor shall be responsible for providing Information System and Service Desk support. The Information System and Service Desk is the single point of contact between 448

SCMW and its Information System customers and is tasked with providing the first line of help to resolve customers’ system administrative and technical problems. The contractor shall document trouble calls made into the Information System Service Desk as trouble tickets via user telephone calls or a web‐based interface. There are two categories of trouble tickets: Routine and VIP/Urgent/Critical. Hours of Operation may vary from 24/7/365 to normal business hours to meet the primary objective to restore normal service to standard operation as quickly as possible in order to minimize adverse impacts on customers, business operations and processes.

The contractor shall receive, document, assign, troubleshoot, resolve, report and track to completion all end user, Information System issues using a documented process. The contractor shall respond to the appropriate functional advocate when deficiency is resolved and testing needs to be accomplished by the individual who identified the bug. The contractor shall collect information for service requests through the Information System Service Desk support management tool and via telephone or e‐mail as appropriate. The contractor shall respond to all problem calls and which may include interface to higher level organizations and/or personnel, warranty service providers, or external software vendors. The contractor shall track all open support tickets to resolution. The contractor shall provide monthly statistics and status reports in the format directed by the Contracting Officer Representative. The contractor shall analyze reported issues and other data to determine trends in problem areas. The contractor shall maintain information on methods used to resolve previous incidents or create a record for future reference if the incident has not been experienced previously. The contractor shall coordinate with applicable technical support staff which may be located in higher or other

organizations. The contractor shall escalate and track issues that are out of the scope of the 448 SCMW-Hill to resolve with the 75 Air Base Wing, and other AFMC and DISA organizations. The contractor shall provide necessary research, analysis and coordination with support staff while documenting the findings and events as part of the trouble ticket prior to escalation. The contractor shall analyze and determine affected community and ensure proactive notification to affected user community with 1 business day using e‐mail, voice mail Web posting and front‐end telephone system postings.

# Service Desk support

The contractor shall facilitate in and out processing of 448 SCMW-Hill employees (civilian, contractor and military). The contractor shall provision network accounts, work with security office to ensure all cybersecurity requirements are completed and provide/maintain a checklist(s) of other in and out-processing tasks to cover each organization and staff

office. Documentation will be maintained in Electronic Records Management (ERM). The contractor will provision and deprovision network accounts through the Enterprise Services Dashboard (IAO Express) and if required, work with the 75 ABW/SC to resolve account issues. The contractor will also review noncompliance reports provided by IAO Express and address identified issues on a monthly basis. The contractor will be responsible to

file share folder permissions located in the Hill Enterprise Data Center (HEDC) and distribution lists located in the Global Access Listing (GAL). The contractor is not responsible for repairing equipment (desktop or laptop) unless it is returned by the ABW services technicians for warranty issues.

# Agent of the Certifying Authority (ACA) Support Services

**ACA support services requirements must comply with applicable documents and standards specified in Section 8 of this PWS.**

The contractor shall provide support services for organization owned systems/servers seeking assistance in obtaining Information System Certification & Accreditation, to include systems (GOTS/COTS) hosted in the cloud. Capabilities include both testing and validating functions of implemented IA controls, functions that may potentially overlap with existing IAM/IAO personnel functions assigned to Information Systems (ISs).

Contractor shall develop and implement of management, operational, and technical security controls required to assure desired levels of protection for systems and data are achieved (e.g., establishment of policy/procedures in support of Federal security requirements, conduct risk assessments to identify threats/vulnerabilities for existing/planned systems; support Federal mandates for measuring and reporting compliance, perform certification and accreditation (C&A) activities; provide training services to promote awareness and knowledge of compliance responsibilities for Federal IT security requirements. The contractor shall ensure that a valid authority to operate (ATO) is maintained for information systems. Contractor shall ensure latest security mandates and implement, which include risk management framework and DISA security technical implementation guide. Contractor shall hold regular periodic information system reviews to ensure compliance standards are maintained. The contractor shall track any identified findings to resolution. The contractor shall develop Plan of Action and Milestones to track work towards a finding to completion and file that information with system security control documents. Contractor shall document system and network security in a government directed documents to include, system security plan, Information Support Plan, Cybersecurity Strategy and changes to the system with regards to security and develop plan of action and milestones for fixes that are in work.

* ACA support with IAM/IAO functions seeking an authority independent of the program to perform both testing and validating of any existing IS security controls put in place by the IS developers. If mitigations to remaining IS vulnerabilities are required, the ACA possesses the necessary skills to recommend additional security controls for program personnel to implement so that the ACA could subsequently re-test and validate.
* ACA support without IAM/IAO functions seeking an authority independent of the program to perform validation of security controls implemented and tested by IAM/IAO personnel before the AF-CA can certify the IS for accreditation at the appropriate Designated Accrediting Authority (DAA).

# Video Teleconference Support

The contractor shall schedule and coordinate all Integrated Services Digital Network (ISDN) and Internet Protocol (IP) based VTCs based on senior leader requirements. The contractor shall dial in VTC within the scheduled window and trouble shoot connection issues if they arise. The contractor shall assist with the design of new system if required, maintain system drawings to include hardware, software and network aspects. The contractor shall work with the 75 ABW/SC to ensure all VTCs are registered correctly according to AF guidelines and maintain an Authority to Operate.

# Equipment Custodian

The contractor must provide support related to Automatic Data Processing Equipment (ADPE) to include, arranging delivery of new equipment from the IT Depot at Hill AFB to the appropriate location (typically, building 1209 on Hill AFB), delivery of equipment to new employees, replace failed equipment for current employees and track equipment and prepare required documentation based on AFI 17-1203 and other specific guidance published by the 75

ABW. The contractor shall complete an annual inventory of all equipment. This will include monitors, external hard drives and mobile devices such as IPhones and IPads. The contractor shall sanitize hard drives IAW standard security policy prior to sending to DRMO or

disposing of them. Contractor will reuse excess equipment as applicable. As part of the tracking actions, contractor will maintain a current map that shows the location of accountable items, which include desktops, laptops, IP phones, printers, monitors and wireless headsets. The map shall be updated based on user moves and when equipment is replaces. The government shall have access to this map at any time. The contractor shall maintain warranty and license information for all hardware and its associated software and work with the manufacturer or reseller to replace/repair equipment as needed.

# Equipment Technical Support

The contractor shall load host base provided image to mobile devices and desktops. The contractor shall add the mobile device or desktop to the domain after the image is applied. The contractor shall replace equipment that has failed/beyond repair, as determined by the ABW installation technician, with new or used equipment. The contractor shall complete the process for warranty repair/replacement if the hardware is within the manufacturer warranty period. The contractor shall troubleshoot unique technical issues with equipment when requested via email or ticket by the ABW technicians. If the issue is resolved, the contractor shall document the resolution in the ticket.

The contractor maintains a stock of hardware (desktops and laptops) that are imaged and ready for deployment in case of equipment failure. The minimum stock required is eight desktops and five laptops.

The contractor shall maintain mobile devices that may be checked out for Temporary Duty (TDY) or other mission requirements. The contractors shall track information related to the checkout including, employee name, organization, pick up date, return date and duty

location. The contractor shall work with the employee to complete the DD Form 4394 and DD Form 1297 when the employee checks out a mobile device. The contractor shall file these forms in the official Electronic Records Management (ERM) folder. The contractor shall contact employees who have not returned return the mobile device within 10 business days of the return date. The contractors shall provide an encrypted mobile device when requested or at a minimum when the employee is travelling OCONUS.

The contractor shall maintain an offline machine for the purpose of flash media transfers. The contractor shall ensure that the machine is compliant with the appropriate regulations.

1. **ENGINEERING REQUIREMENTS**
   1. **Systems Engineering**
      1. **Life-Cycle Systems Engineering**

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

# Architecture and System Design

The contractor shall support the design and development of systems and applications and their integration into the overarching enterprise architecture. The contractor shall provide all required design and development documents, and supporting architectural documentation, for any frameworks as identified in this task order.

# Department of Defense Architectural Framework (DoDAF) Guidance

The contractor shall provide all required design and development documents, and supporting architectural documentation in compliance with the latest Department of Defense Architectural Framework (DoDAF) Enterprise Architecture

guidance <http://dodcio.defense.gov/Portals/0/Documents/DODAF/DoDAF_v2-02_web.pdf>.

# Configuration Management

The contractor shall accomplish Configuration Management (CM) activities as described in the task order.

# Testing

* + 1. **Product/System Integration Testing**

The contractor shall perform testing and inspections of all system services to ensure the technical adequacy and accuracy of all work, including reports and other documents required in support of that work. The contractor shall conduct on-site testing when requested. When specified by the Government, the contractor shall participate with the Government in testing the complete system or application which may include premise equipment, distribution systems or

any additional telecommunications equipment or operating support systems identified in the task order. After appropriate corrective action has been taken, all tests including those previously completed related to the failed test and the corrective action shall be repeated and successfully completed prior to Government acceptance. Pre-cutover audits will consist of verification of all testing completed by the contractor such that the system is deemed ready for functional cutover. As part of this audit, any engineered changes or approved waivers applicable to the installation will be reviewed and agreed upon between the contractor and the Government. Post-cutover audits will verify that all post-cutover acceptance testing has been performed satisfactorily IAW the standard practices and identify those tests, if any, which have not been successfully completed and must be re-tested prior to acceptance. Testing shall be performed in two steps: operational testing, then system acceptance testing. The contractor shall provide a logical test process that minimizes interruptions and avoids sustained downtime and presents a contingency procedure to be implemented in the event of systems failure during testing.

# Simulated Operational Testing

The contractor shall conduct testing ranging from data entry and display at the user level combined with system loading to represent a fully operational system. The contractor shall accomplish operational testing IAW the contractor-written, Government-approved test plan as specified in the task order. The plan shall consist of a program of tests, inspections and demonstrations to verify compliance with the requirements of this Task Order. The

contractor shall document test results in the test report(s). The contractor shall be responsible track deficiencies until they are resolved.

# Acceptance Testing

The contractor shall provide on-site support during the acceptance-testing period. Acceptance testing shall be initiated upon acceptance of the operational test report and approval of the acceptance test plan. This on-site support shall be identified in the acceptance test plan.

# System Performance Testing

The contractor shall provide system performance testing. The acceptance test will end when the system or application has maintained the site-specific availability rate specified in this task order. In the event the system or application does not meet the availability rate, the acceptance testing shall continue on a day-by-day basis until the availability rate is met. The contractor shall perform diagnostics on database and server performance to support the ability to show improvements or degradation in performance.

# Information Assurance

The contractor shall ensure that all system deliverables meet the requirements of DoD and AF Information Assurance (IA) policy. Contractor shall sign/approve DD form 2875 for access to organization owned information systems and network. Furthermore, the contractor shall ensure that personnel performing IA activities obtain, and remain current with, required technical and/or management certifications.

# System IA

For those solutions that will not inherit existing network security controls, and thus integrate an entirely new application system consisting of a combination of hardware, firmware and software,

system security assurance is required at all layers of the TCP/IP DoD Model. The contractor shall ensure that all system deliverables comply with DoD and AF IA policy, specifically

DoDI 8500.2, *Information Assurance Implementation*, and AFI 17-130, Cybersecurity Program Management. To ensure that IA policy is implemented correctly on systems, contractors shall ensure compliance with DoD and AF Certification & Accreditation policy, specifically

DoDI 8510.01, *DoD Information Assurance Certification and Accreditation Process (DIACAP)*, and AFI 17-101, Risk Management Framework (RMF for Information Technology. The contractor shall also support activities and meet the requirements of DoDI 8520.02, *Public Key Infrastructure (PKI) and Public Key (PK) Enabling,* in order to achieve standardized, PKI- supported capabilities for biometrics, digital signatures, encryption, identification and authentication.

Contractor shall ensure availability, integrity, authentication, confidentiality and non‐repudiation of information and information systems (IS) owned by the organization. This includes data protections, detection and restoration of data. Contractor shall ensure that information systems are updated with the latest security software and patches. Contractor shall ensure that information systems, hardware and software maintain the correct certification and accreditations before using them on the network. Contractor shall implement technical and security

notices and mandates received from higher headquarters. Contractor will troubleshoot and monitor the success of HQ AFMC SMS pushes, create patch and software distribution packages, provide the ability to query client systems for current SDC versions, hardware and driver compatibility and maintain system security and integrity. Contractor shall limit access to files and programs to authorized personnel only as designated by the security manager and government senior leadership.

# Personnel IA

Personnel performing Information Assurance (IA) activities are required to obtain, and remain current with, technical and/or management certifications to ensure compliance with DoD 8570.01-M, *Information Assurance Workforce Improvement Program*, 19 December 2005 (with all current changes).

# CONTRACTUAL REQUIREMENTS

* 1. **Place of Performance**

Work shall be performed at the customer (Government) site. Travel to other Government or contractor facilities may be required in support of duties outlined in this PWS

# Normal Hours of Operation

Normal core hours are 8:00 am to 4:30 pm, Monday thru Friday (excluding federal holidays, contractor employee(s) vacation and sick leave, base closure days, etc.), eight (8) hours per day, forty (40) hours per week. The contractor may use flexible hours for start and end time. Flexible hours are 7:00 am to 8:30 am and 3:30 pm to 5:00 pm. Government surveillance of contractor performance is required to give reasonable assurance that efficient methods and effective cost controls are being used. Telework is authorized on this contract; however, it must be coordinated and approved through the Contracting Officer Representative and be in the best interest of the government.

# Overtime Requirements

There is an over and above CLIN that may be used in the event that there is a cybersecurity related event that needs to be resolved. Specifically, the tasks should be related to paragraphs 3.5 and 3.4.2. In order to use the funding, the contractor shall provide a statement in writing with the individual’s name who will be working the over time, date, estimated number

of hours, issue and mitigation plan to the Contracting Officer Representative for review and final approval by the Contracting Officer.

# Government Furnished Property

The Government will furnish or make available working space, network access and equipment to include:

* Computer with Microsoft Office Suite (Outlook, Word, Excel, PowerPoint, etc.)
* Telephone (local/long distance calls authorized as dictated by Task Order performance requirements)
* Facsimile
* Copier
* Printer

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

The contractor shall conduct a joint inventory and turn in this equipment to the COR upon request or completion of the Task Order.

# Billable Hours

In order for man-hours to be billed, deliverable services must have been performed in direct support of a requirement in the PWS. In the course of business, situations may arise where Government facilities may not be available for performance of the requirements (i.e.,

base closure due to weather, Force Protection conditions, etc.). When the base is officially closed no contractor services will be provided and no charges will be incurred and/or billed to any service. There may also be occasions when support contractors are invited to participate in morale and recreational activities (i.e., holiday parties, golf outings, sports days and other various social events). Contractor employees shall not be directed to attend such events by the Government. Since a contract employee is not a government employee, the contract employee cannot be granted the same duty time activities as Government employees. Participation in such events is not billable to the TO and contractor employee participation should be IAW the employees’ company’s policies and compensation system.

# Non-Personal Services

The Government will neither supervise contractor employees nor control the method by which the contractor performs the required tasks. Under no circumstances shall the

Government assign tasks to, or prepare work schedules for, individual contractor employees. It shall be the responsibility of the contractor to manage its employees and to guard against any actions that are of the nature of personal services or give the perception of personal

services. If the contractor feels that any actions constitute, or are perceived to constitute personal services, it shall be the contractor’s responsibility to notify the Task Order (TO) Contracting Officer (CO) immediately. These services shall not be used to perform work of a policy/decision making or management nature, i.e., inherently Governmental functions. All decisions relative to programs supported by the contractor shall be the sole responsibility of the Government. These operating procedures may be superseded by Theater Commander’s direction during deployments.

# Contractor Identification

All contractor/subcontractor personnel shall be required to wear an AF-approved or provided picture identification badges above the waist so as to distinguish themselves from Government employees. When conversing with Government personnel during business meetings, over the telephone or via electronic mail, contractor/subcontractor personnel shall identify themselves as such to avoid situations arising where sensitive topics might be better discussed solely between Government employees. Contractors/subcontractors shall identify themselves on any attendance sheet or any coordination documents they may review. Electronic mail signature blocks shall identify their company affiliation. Where practicable, contractor/subcontractors occupying collocated space with their Government program customer should identify their work space area with their name and company affiliation. ***Refer to Clause H063 of the overarching ID/IQ contract.***

# Performance Reporting

The contractor’s task order performance will be monitored by the Government and reported in Contractor Performance Assessment Reports (CPARs) or a Customer Survey, depending on the dollar amount of the task order. Performance standards shall include the contractor’s ability to provide or satisfy the following:

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

# Program Management/Project Management

The contractor shall identify a Program Manager or a Project Manager who shall be the primary representative responsible for all work awarded under this task order, participating in Program/Project Management Reviews and ensuring all standards referenced herein are adhered to. The Program/Project Manager shall facilitate a quarterly Lessons Learned/Program Management Review with all contractors and government team.

# Services Delivery Summary

***Reference Section 6,* Services Delivery Summary*, of this PWS for specific performance objectives.***

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

# Task Order Management

The contractor shall establish and provide a qualified workforce capable of performing the required tasks. The workforce may include a project/task order manager who will oversee all aspects of the task order. The contractor shall use key performance parameters to monitor work performance, measure results, ensure delivery of contracted product deliverables and solutions, support management and decision-making and facilitate communications. The contractor shall maintain a risk management plan to facilitate the following tasks: identify risks, resolve problems and verify effectiveness of corrective actions. The contractor shall institute and maintain a process that ensures problems and action items discussed with the Government are tracked through resolution and shall provide timely status reporting. Results of contractor actions taken to improve performance shall be tracked and lessons learned incorporated into applicable processes. The contractor shall establish and maintain a documented set of disciplined, mature and continuously improving processes for administering all contract efforts with an emphasis on cost-efficiency, schedule, performance, responsiveness and consistently high-quality delivery. The contractor shall provide a staffing plan, communication plan and transition plan prior to contract award. If an employee leaves, the contractor shall provide the COR an updated staffing plan with details on how the position will be filled within 10 business days of the employee leaving. The communication plan shall be updated on an annual basis.

The contractor shall provide a monthly status report within 10 calendar days of the following month that details projects in work. The government retains the right to request and/or modify the current format at no additional cost to the government.

The Contractor shall assist with transition of workload. Examples of transition activities may include status briefings or demonstrations of current workload being performed to other Government employees. In the event a follow-on contract is awarded to other than the incumbent Contractor or if the operation reverts to in-house, the incumbent Contractor shall provide all reasonable support to the government and/or the successful offeror to ensure an orderly transition and minimize any impact on the entire operation. The successful offeror shall also provide a transition plan to ensure the successful transition of tasks outlined in this PWS.

# Documentation and Data Management

The contractor shall provide the Government with electronic access to the following data, including access to printable reports: CDRLs, White Papers, Status Reports, Audit Reports, Agendas, Presentation Materials, Minutes, Contract Letters and Task Order Proposals. The contractor shall provide the Government with electronic access to this data, including access to printable reports.

# Records, Files, and Documents

All physical records, files, documents and work papers, provided and/or generated by the Government and/or generated for the Government in performance of this PWS, maintained by The contractor which are to be transferred or released to the Government or successor contractor, shall become and remain Government property and shall be maintained and

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

# Personnel Security

Individuals performing work under this PWS shall comply with applicable program security requirements as stated. This PWS includes Unclassified; Unclassified, But Sensitive and Secret

(S) work.

Contractors shall be able to obtain adequate security clearances prior to performing services under the task order. The Contract Security Classification Specification (DD Form 254) will be at the basic contract and task order level and will encompass all security requirements. All contractors located on military installations shall also comply with Operations Security (OPSEC) requirements as set forth in DoD Directive 5205.02, Operations Security Program and AFI 10- 701, Operations Security. In accordance with DoD 5200.2-R, Personnel Security Program (Jan 87), DoD military, civilian, consultants and contractor personnel using unclassified automated information systems, including e-mail, shall have, at a minimum, a completed favorable National Agency Check plus Written Inquiries (NACI).

The types of Personnel Security Investigations (PSI) required for The contractor vary in scope of investigative effort depending upon requirements of the Government and/or conditions of the Task Order. In cases where access to systems such as e-mail is a requirement of the Government, application/cost for the PSI shall be the responsibility of the Government. In cases where access to systems is as a condition of the Task Order, application/cost for the appropriate PSI shall be the responsibility of The contractor. In such

instances, The contractor shall diligently pursue obtaining the appropriate PSI for its employees prior to assigning them to work any active task order. Acquisition planning must consider Anti- Terrorism (AT) measures when the effort to be contracted could affect the security of operating forces (particularly in-transit forces), information systems and communications systems

IAW DoD Instructions 2000.16 Anti-Terrorism Standards.

# Transmission of Classified Material

The contractor shall transmit and deliver classified material/reports IAW the National Industrial Security Program Operating Manual (DoD 5220.22-M). These requirements shall be accomplished as specified in this task order.

# Protection of System Data

Unless otherwise stated in the task order, The contractor shall protect system design-related documents and operational data whether in written form or in electronic form via a network in accordance with all applicable policies and procedures for such data, including DoD Regulation

5400.7-R and DoD Manual 5200.01(v1-v4) to include latest changes, and applicable service/agency/combatant command policies and procedures. The contractor shall protect system design related documents and operational data at least to the level provided by Secure Sockets Layer (SSL)/Transport Security Layer (TSL)-protected web site connections with certificate and or user ID/password-based access controls. In either case, the certificates used by The contractor for these protections shall be DoD or IC approved Public Key Infrastructure (PKI) certificates issued by a DoD or IC approved External Certification Authority (ECA) and shall make use of at least 128-bit encryption.

# System and Network Authorization Access Requests

For contractor personnel who require access to DoD, DISA or Air Force computing equipment or networks, The contractor shall have the employee, prime or subcontracted, sign and submit a System Authorization Access Report (SAAR), DD Form 2875.

# Travel

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

# Training

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

# Other Government-Provided Training

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

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

# Data Rights and Non-Commercial Computer Software

In order to implement the provisions at DFARS 252.227-7013(b) and (e) and DFARS 252.227- 7014(b) and (e) and DFARS 252.227-7017, The contractor shall disclose to the ordering

Contracting Officer and ordering office in any proposal for a task order, or after award of a task order if not previously disclosed in the proposal, any technical data or non-commercial computer software and computer software/source code documentation developed exclusively at government expense in performance of the task order. This disclosure shall be made whether or not an express requirement for the disclosure is included or not included in the PWS or solicitation for the order. The disclosure shall indicate the rights asserted in the technical data and non-commercial computer software by the contractor and rights that would be acquired by the government if the data or non-commercial software was required to be delivered under the task order and its CDRL requirements and any cost/price associated with

delivery. Performance of this disclosure requirement shall be considered a material performance requirement of any task order under which such technical data or non-commercial computer software is developed exclusively at Government expense.

# Software Support and Data Rights

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

# Manuals and Supplemental Data

The contractor shall provide documentation for all systems services delivered under this Task Order. This documentation shall include users’ manuals, operators’ manuals, maintenance manuals and network and application interfaces if specified in the task order.

# Transition and Decommissioning Plans

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

448 SCMW-Hill is in the process of transitioning information technology services and

support to other organizations and/or higher levels of service support and the contractor shall provide support during the transition until responsibility has been subsumed by the gaining organization.

# Section 508 of the Rehabilitation Act

The contractor shall meet the requirements of the Access Board’s regulations at 36 CFR Part 1194, particularly 1194.22, which implements Section 508 of the Rehabilitation Act of 1973, as amended. Section 508 (as amended) of the Rehabilitation Act of 1973 (20 U.S.C. 794d) established comprehensive requirements to ensure: (1) Federal employees with disabilities are able to use information technology to do their jobs, and (2) members of the public with disabilities who are seeking information from Federal sources will be able to use

information technology to access the information on an equal footing with people who do not have disabilities.

# Continuation of Essential Contractor Services During Crisis Declared by the President of the United States, the Secretary of Defense, or Overseas Combatant Commander

The performance of these services may be considered mission-essential functions during time of crisis. Should a crisis be declared by the Secretary of Defense, the CO or representative will verbally advise The contractor of the revised requirements, followed by written direction. When a crisis is declared, limited services identified in this PWS are considered mission-essential functions during a crisis. The only service considered mission essential is server administration listed under paragraph 3.4.2. The contractor shall continue providing service to the requesting organization 24-hours a day until the crisis is over. The contractor shall ensure enough skilled personnel are available during a crisis for any operational emergency. A crisis management plan shall be submitted IAW A-TE-3, A04, which states that the contractor shall “Submit an essential personnel list within 10 days after the contract start date.” The list shall contain the employee’s name, address, home phone number, cell phone number, security clearance and duty title. This list shall be updated annually or as changes occur. It must include the language spelled out in DFARS 237.76 – Continuation of Essential Contractor Services to identify services determined mission-essential functions during a crisis situation IAW DODI

3020.37. **Note: It is the responsibility of the Combatant Commander to determine mission-essential functions and to establish procedures to ensure that these standard support requirements and any additional requirements are met.**

* 1. **Safety Voluntary Protection Program**
     1. **Definitions**

Applicable Contractors-The following Voluntary Protection Program (VPP) requirements apply only to Contractors whose employees perform work of more than one thousand (1000) hours per yearly quarter on a Government installation.

Days Away, Restricted, and or Transfer Case Incident Rate (DART). -The number of recordable injuries and illness cases per one hundred (100) full-time employees resulting in days away from work, restricted work activity, and/or job transfer that a site has experienced in a given time frame.

Total Case Incident Rate (TCIR) -The total number of recordable injuries and illness cases per one hundred (100) full-time employees that a site has experienced in a given time frame.

# Impact

VPP impacts all applicable Contractors operating on AF Installations. It is the Contractor's responsibility to ensure its Contractor employees and managers have a comprehensive understanding of VPP as well as full compliance with OSHA requirements. Contractors shall follow the safety and health rules of the installation and OSHA. Detailed information on VPP is available on the OSHA website at <http://www.osha.gov/dcsp/vpp/index.html>.

# Rates

The Contractor shall submit their TCIR, DART rates, and OSHA Form 300A annually to contracting officer for consolidation and submission as part of the installation's annual

VPP Safety and Health management report. TCIR and DART rates are due by the 15th of

January of each year. Should the contract expire before January 15th, the Contractor shall submit their TCIR, DART rates, and OSHA Form 300A by the end of the contract PoP.

# OSHA Compliance

The Contractor shall be responsible for compliance with the OSHA (Public law 91-596). The Contractor shall submit a Safety and Health Plan and corresponding site safety checklist to the contracting officer ten (10) business days after individual task order awards. Reference Appendix C for additional details. The Contractor's Health and Safety plan shall include appropriate measures to ensure the Contractor reacts promptly, to investigate, correct and track alleged safety and health violations and uncontrolled hazards in the Contractor work areas. The plan shall include the following:

* The Contractor shall demonstrate a management commitment to employee safety and health.
* The Contractor shall identify the application of the safety and health plan to sub- Contractors/team members.
* The Contractor’s Safety and Health Plan shall identify the roles and responsibilities of the management, supervisors, Contractor employees and the safety coordinator.
* The Contractor shall identify applicable safety rules and regulations.
* The Contractor shall include a worksite hazard analysis to include base-line hazard identification and required control measures.
* The Contractor shall include a job site analysis to include hazards of tasks required to control measures.
* The Contractor shall identify Contractor employee safety and health training requirements and the documentation process.
* The Contractor shall include a workplace inspection frequency, to include identifying the Contractor employee conducting the inspections.
* The Contractor shall include employee hazard and mishap reporting procedures.
* The Contractor shall identify Contractor employee(s) responsible for corrective hazards.
* The Contractor shall identify first aid and injury procedures.
* The Contractor shall identify procedures for accident investigation and reporting.
* The Contractor shall identify emergency response procedures.
* The Contractor shall identify the process for tracking controlled hazards in Contractor work areas.

# Sub-Contractors

The Contractor shall be responsible for establishing these requirements for all sub- contractors/team members who qualify as applicable Contractors.

# Contractor Manpower Reporting

The contractor shall report ALL contractor labor hours (including subcontractor labor hours) required for performance of services provided under this contract for the 448 SCMW via a secure data collection site. The contractor is required to completely fill in all required data fields at [https://www.ecmra.mil](https://www.ecmra.mil/)

Reporting inputs will be for the labor executed during the period of performance for each Government fiscal year (FY), which runs 1 October through 30 September. While inputs may be reported any time during the FY, all data shall be reported no later than 31 October of each calendar year. Contractors may direct questions to The contractor Manpower Reporting Application (CMRA) help desk.

Notes:

*Reporting Period:* Contractors are required to input data by 31 October of each year. However, due to the delayed implementation, input of FY12 data is required by 31 Mar 13.

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

with the contractor name and contract number associated with the data.

*User Manuals:* Data for Air Force service requires must be input at the Air Force CMRA link. However, user manuals for government personnel and contractors are available at the Army CMRA link at [http://www.ecmra.mil](http://www.ecmra.mil/)

# SERVICES DELIVERY SUMMARY

|  |  |  |
| --- | --- | --- |
| **PWS**  **Paragraph** | **Performance Objective / Elements** | **Standards** |
|  | *Information Technology* |  |
| 3.4.2 | System availability is restored within 2-4 hours of identification of issues. If not restored, The contractor must provide feedback and ECD to MSDIS and LD2RMS PMs. 95% availability except  scheduled downtime | Contractor shall  ensure LD2RMS and MSDIS are available 99% of the time. |
| 3.5 | Maintain RMF compliance IAW applicable DoD and AF policy and instruction | Contractor shall complete required activities to ensure compliance. |
| 3.6 | No more than 1 VTC per quarter is not  arranged/ dialed in | Contractor shall ensure VTCs are  arranged and dialed in on time. |
| 3.7 | Annual Inventory with less than 1% of accountable items missing | Contractor shall complete an annual inventory. |

|  |  |  |
| --- | --- | --- |
|  | ***MSDIS*** |  |
| 3.1 | Report any security issues with 48 hours  of discovery | Contractor shall report security  issues. |
| 3.1 | Severity Code 1/2 tickets are assigned within 4 hours of receiving them. Note: PM and Functional Advocates will assist and inform Contract Manager if there is  a hot ticket. | Contractor shall assign high severity tickets in a timely manner. |
| 3.1 | Issues dealing with security or compliance (FISMA, NDAA, CCA) will be worked with higher priority or in  conjunction to functional module priorities. | Contractor shall correct security and compliance issues as the higher priority. |
| 3.1 | Complete 2 Sustainment tickets per month per module | Contractor shall complete a  minimum of 2 Sustainment tickets a month. |
| 3.2 | Complete 2 Dev/Mod tickets per month per module | Contractor shall complete a minimum of 2 Dev/ Mod tickets a  month. |
| 3.1, 3.2 | Provide estimate time to program on all  assigned tickets | Contractor shall provide estimated  time to program. |
| 3.1, 3.2 | High priority bugs involving will be resolved within two business days of official request. If the bug cannot be resolved, then an action plan and workaround will be coordinated  between The contractor and the government. | Contractor shall resolve Severity 1 and 2 or other high priority issues |
| 3.1, 3.2 | Development is complete to the specification in the government provided detailed requirements document.  Determination will be made by the functional advocate or program manager | Contractor shall complete development requirements based on approved Computer System Requirement Documents |
| 3.1, 3.2 | Based on 100% inspection prior to code  release, functionality will go through development and security testing. | Contractor will send tickets through the COR/PM prior to code release |
| 3.3.10 | Requested data/report/requirements analysis is provided to the government  within three business days of official request | Contractor will provide data and requirements support |
|  | ***LD2RMS*** |  |
| 3.1 | High priority bugs involving will be resolved within two business days of official request. If the bug cannot be resolved, then an action plan and workaround will be coordinated between The contractor and the  government*.* | Contractor shall resolve Severity 1 and 2 or other high priority issues |

|  |  |  |
| --- | --- | --- |
| 3.1 | Based on 100% inspection prior to code  release, functionality will go through development and security testing. | Contractor will send tickets through the COR/PM prior to code release |
|  | ***General Contract Requirements*** |  |
| 5.8.2 | Communication | Report any problems with PWS task  completion to the COR within 48 hours of when the problem started |
| 5.8.2 | Monthly Status Report | Contractor shall submit MSRs to the CORs within 24 hours of the due date (10th of each month) with no more than 2 significant  errors. Errors shall be corrected within 5 business day after notification. |

1. **SECURITY REQUIREMENTS**

***Security requirements are detailed in the DD254.***

# Personnel Security Clearance Requirements

Some or all of the personnel performing work on this contract will require a security clearance as identified below:

# (X) Secret

The contractor shall request security clearances for personnel requiring access to classified information within 15 business days after receiving a facility clearance or,

if the contractor is already cleared, within 15 business days after service award. Due to costs involved with security investigations, contractor security clearances shall be kept to an absolute minimum necessary to perform service requirements. Contractors will elevated or administrative privileges to the network or a specific server(s) shall have a secret clearance.

# Additional Investigation Requirements

Anyone working on the contract that does not require a security clearance must have at a minimum a favorably adjudicated National Agency Check with Written Inquiries (NACI) investigation to access a government furnished information system or environment. This investigation must be submitted by the contract company. Note: AFI 31-501, and AFI 31-601 for unescorted entry to restricted areas, access to sensitive unclassified information, access to government automated information systems (AIS) and/or sensitive equipment.

# Security Manager Appointment

The contractor shall appoint a security manager for the on base long-term visitor group. The security manager may be a full-time position or an additional duty position. The security manager shall provide contractor employees with training required by DoDM 5200.01, Volume 3, Enclosure 5, *DoD Information Security Program*, AFPD 31-4, *Information Security* and AFI 31-401, *Information Security Program Management*. The contractor security manager shall provide initial and follow-on training to contractor personnel who work in Air Force controlled or restricted areas. Air Force restricted and controlled areas are explained in AFI 31-101, *Air Force Integrated Defense Plan*.

# Visit Requests

Contractors participating in the National Industrial Security Program are authorized to use Joint Personnel Adjudication System (JPAS) in lieu of sending Visitor Authorization Letters (VALs) for classified visit to Department of Defense facilities and military installations. VALs are only required if the contractor isn’t using JPAS or if contractor personnel whom access level and affiliation are not accurately reflected in JPAS. However, some agencies may still require VALs to be submitted for access to their facilities. Visit requests must be sent to servicing government’s security management office (SMO) code. Each contractor performing work on the contract will require a separate SMO Code visit request from the contactor. The visit request must include all prime and subcontract workers on the contract.

# Obtaining and Retrieving Identification Media

As prescribed by the AFFAR 5352.242-9000 Contractor Access to Air Force Installations, AFFAR 5352.242-9001, Common Access Cards (CAC) for Contractor Personnel and FAR 52.204-9, Personal Identity Verification of Contractor Personnel, The contractor must comply with the requirements set forth in these guidance. Contractors requesting a CAC for

personnel on the contract will submit on company letterhead the names and all other personnel information as prescribed by the contracting officer to begin the identification processing

effort. Contracting officers will follow installation specific guidance regarding the issuance and recovery of all identification media issued to The contractors by the government. Failure to return all government issued identification upon termination of contract or service, termination of employees or expiration of the identification may result in withholding of final payment.

# Pass and Identification Items

The contractor shall ensure the following identification items as required for contract performance are obtained for employees:

* DoD Common Access Card (AFI 36-3026).

Failure to return all government issued identification upon termination of contract or service, termination of employees or expiration of the identification may result in withholding of final payment.

# Information Security

The contractors performing duties associated with this task order must adhere to all the standards for protecting classified information as specified in DoDM 5200.01, Volumes 1- 4, *DoD Information Security Program*, Air Force Instruction 31-401, *Information Security Program Management* and all applicable supplements and operating instructions.

# Unescorted Entry to Secure Rooms

Contractor personnel requiring unescorted entry to secure rooms designated by the installation commander shall comply with base access requirements and these additional security instructions; DoD 5200.2-R, *DoD Personnel Security Program,* AFI 31-101, *Air Force Integrated Defense Plan* and AFI 31-501, *Personnel Security Program Management* as

applicable. Contractor personnel shall be the subject of a favorably adjudicated National

Agency Check with Local Agency Check (NACLC) investigation to qualify for unescorted entry to a secure room. Contractor personnel must contact their Contracting Officer Representative (COR) and the appropriate secure room monitor for permission.

# Computer and Network Access Requirements

Contractor personnel working on this contract must be designated in one of the below AIS positions and complete the required security investigation to obtain the required security clearance. This must be accomplished before operating ***government furnished*** computer workstations or systems that have access to ***Air Force*** e-mail systems or computer systems that access classified information. The contractor shall comply with the DoD 5200.2-

R, *Personnel Security Program* and AFMAN 33-152, *User Responsibilities and Guidance for Information Systems*, requirements. Position requirements will be determined based on the position. Those with elevated privilege the Air Force network will be required to maintain a secret clearance.

**(X) AIS-II Position - Noncritical-Sensitive Positions. Security Clearance: SECRET** Based on a NACLC/ANACI background investigation. Responsibility for systems design, operation, testing, maintenance and/or monitoring that is carried out under technical review of higher authority in the AIS-I category, includes, but is not limited to; access to and/or processing of proprietary data, information requiring protection under the Privacy Act of 18 1974 and Government-developed privileged information involving the award of.

**(X) AIS-III Position - Nonsensitive Positions.** No security clearance required but is a **Trusted Position** based on a favorable NACI background investigation. All other positions involved in U.S. Government computer activities.

# Reporting Requirements

The contractor shall comply with requirements from AFI 71-101*,* Volume-1

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

# Physical Security

Contractor employees shall comply with base Operations Plans/instructions for FPCON procedures, Random Antiterrorism Measures (RAMS) and Operation Security (OPSEC), Emergency Management (EM) and local search/identification requirements. The contractor shall safeguard all government property including controlled forms provided for contractor use. At the close of each work period, government training equipment, facilities, support equipment and other valuable materials shall be secured.

# Operating Instructions

The contractor will adhere to the all Air Force activity Operating Instructions (OI) and local Security Program Management for internal circulation control, protection of resources and to regulate entry into Air Force controlled areas during normal, simulated and actual emergency operations to include local written OIs.

# Government Authorization

The contractor shall ensure its employees do not allow government issued keys to be used by personnel other than current authorized contractor employees. Contractor employees shall not use keys to open work areas for personnel other than contractor employees engaged in performance of duties, unless authorized by the government functional director.

# Access Lock Combinations

Access lock combinations are “*For Official Use Only”* and will be protected from disclosure to unauthorized personnel. The contractor will adhere to the Air Force activity operating instructions ensuring lock combinations are not revealed to un-cleared /unauthorized persons and ensure the safeguard procedures are implemented. The contractor is not authorized to record lock combinations without written approval by the government functional director.

# Freedom of Information Act Program (FOIA*)*

The contractor shall comply with DoD Regulation 5400.7-R/Air Force Supplement, *DoD Freedom of Information Act Program,* requirements. The regulation sets policy and procedures for the disclosure of records to the public and for marking, handling, transmitting and safeguarding for *Official Use Only (FOUO)* material. The contractor shall comply with AFI 33- 332, *Air Force Privacy Act Program*, when collecting and maintaining information protected by the Privacy Act of 1974 authorized by Title 10, United States Code, Section 8013. The contractor shall maintain records in accordance with Air Force manual (AFMAN) 33-363, Management of Records; and disposed of in accordance with Air Force Records Information Management System (AFRIMS) Records Disposition Schedule (RDS) located at https:[//www.my.af.mil/g](http://www.my.af.mil/gcss-af61a/afrims/afrims/)cs[s-af61a/afrims/afrims/.](http://www.my.af.mil/gcss-af61a/afrims/afrims/)

# Traffic Laws:

The contractor and their employees shall comply with all installation traffic regulations.

# Cellular Phone Operation Policy

The contractor shall comply with local base policies regarding cellular phone operation.

# Security Education and Training

The contractors are required to participate in the government’s in-house and web-based security training program under the terms of the contract. The government will

provide The contractor with access to the on-line system. Annually, all contractors will complete all required security training. Required annual training includes Force Protection (FP), Information Protection (IP), Cybersecurity and OPSEC. If contract team members will be using the SIPRNet, users will also have to comply with the organizational Derivative Classification Training as a condition of access.

# DATA DELIVERABLES

The Government reserves the right to review all data deliverables for a period of 10 working days prior to acceptance. No data deliverable will be assumed to be accepted by the

Government until the required time has passed, unless the Government explicitly states otherwise in the task order.

The Government requires all deliverables that include Scientific and Technical Information (STINFO), as determined by the Government, be properly marked IAW DoD Directive 5230.24 and AFI 61-204 prior to initial coordination or final delivery. Failure to mark

deliverables as instructed by the Government will result in non-compliance and non-acceptance of the deliverable. The contractor shall include the proper markings on any deliverable deemed STINFO regardless of media type, stage of completeness or method of distribution. Therefore, even draft documents containing STINFO and STINFO sent via e-mail require correct markings. Additionally, as required by individual Task/Delivery Orders, The contractor shall formally deliver as a CDRL all intellectual property, software, licensing, physical records, files, documents, working papers and other data for which the Government shall treat as deliverable. Refer all questions regarding data requirements to the IT Program Manager.

Data Deliverables:

|  |  |  |  |
| --- | --- | --- | --- |
| 3.4.3 | A016 | DI-ILSS-80872 | Training Materials |
| 3.4.3 | A017 | DI-ILSS-81070 | Training Program Development and Management Plan |
| 3.1, 3.2 | A041 | DI-IPSC-81633 | Software Programmer's Guide |
| 3.4.3 | A042 | DI-IPSC-81756 | Software Documentation |
| 5.8.2 | A048 | DI-MGMT-80227 | Contractor's Progress, Status and Management Report |
| 3.2 | A063 | DI-MGMT- 81740A | Software Resources Data Reporting: Final Developer Report and Data Dictionary |
| 5.8 | A064 | DI-MGMT-81797 | Program Management Plan |
| 5.8.2 | A065 | DI-MGMT-81808 | Contractor's Risk Management Plan |
| 5.8.2 | A066 | DI-MGMT-81809 | Risk Management Status Report |
| 5.8.2 | A067 | DI-MGMT-81834 | Contractor's Personnel Roster |
| 5.16 | A099 | DI-MISC-80508  B/T | Safety Plan/Checklist |
| 5.16 | A100 | DI-SAFT-8156/T | Mishap Report |

# APPLICABLE STANDARDS AND REFERENCES

Refer to Appendix A3, “Application Services Standards & References,” for applicable certifications, specifications, standards, policies and procedures that are required for compliance on individual Task Orders. Tailor the list as needed for individual Task Orders may impose additional standards to those required at the contract level. The list is not all-inclusive and the most current version of the document at the time of task order issuance will take precedence. Web links are provided wherever possible.

In addition, the contractor shall comply with regulation specified certification for individuals with elevated rights to the Air Force network. At a minimum, Comptia Security+ is required.

DoD 8570.01 and AFMAN 17-1303 were updated in May 2020 to provide additional clarification on certification requirements for those with elevated rights to the AF network, to include Information System Security Managers, Server Administrators and Software Developers (new requirement). The contractor shall appoint a minimum of one senior software developer per system that will meet the certification requirements.

This contract involves access to Personally Identifiable Information (PII) to support cybersecurity and system development requirements and the contractor shall ensure employees understand proper handling and protection procedures.

The contractor shall maintain CMMI Level 3 certification or equivalent.