



Depot Maintenance Applications Consolidation (DMAC) 3 Performance Work Statement (PWS)

(FA877026RB008)

Version 1.00

EXECUTIVE SUMMARY

The Air Force Materiel Command (AFMC), Air Force Life Cycle Management Center (AFLCMC), Business and Enterprise Systems (BES), Enterprise Logistics Systems Division (GB4), Maintenance and Installation Portfolio (GBM), Wright-Patterson Air Force Base (AFB), has a requirement to consolidate two existing service contracts into a singular effort to improve coordination and management of Information Technology (IT) service delivery. This Performance Work Statement (PWS) describes sustainment and surveillance services in support of the following systems: Depot Maintenance Consolidated Operational Database (DMCODB), Depot Maintenance Systems Integration (DMSI), and Depot Maintenance Legacy Systems (DMLS).

Table of Contents

EXECUTIVE SUMMARY	2
1. INTRODUCTION/PURPOSE.....	7
2. SCOPE	7
3. BACKGROUND.....	7
3.1. Depot Maintenance Systems Integration (DMSI)	7
3.1.1. DMSI Client/Server Applications	7
3.1.2. Depot Maintenance Consolidated Operational Database (DMCODB)	8
3.2. Depot Maintenance Legacy Systems (DMLS)	8
4. REQUIREMENTS/DESCRIPTION OF SERVICES	9
4.1. Skills and Knowledge	9
4.1.1. General Skills and Knowledge	9
4.1.2. DMSI Support Skills and Knowledge.....	10
4.1.3. DMCODB Support Skills and Knowledge	10
4.1.4. DMLS Support Skills and Knowledge	11
4.2. Program Management Plan.....	12
4.3. Contractor Responsibilities and Support	13
4.4. Contractor Transition Support.....	14
4.4.1. Initial Kickoff Meeting.....	14
4.4.2. Contract Start	14
4.4.3. Contractor Transition and Decommissioning Plans	15
4.4.4. Transition at Contract Conclusion	15
4.4.5. Transition Working Group (TWG).....	16
4.5. Data Analysis	16
4.6. Enterprise Management Support	17
4.7. Systems Support	17
4.8. Development, Test, Training and Production Servers.....	17
4.9. Agile / Incremental Delivery Methodology.....	18
4.9.1. Current Sustainment and Maintenance	18
4.9.2. Surge Requirements	18
4.10. Specific Task Descriptions	19
4.10.1. Database Integration and Design.....	19
4.10.2. Data Conversion	20

4.10.3.	Interface Software Design and Maintenance	21
4.10.4.	Interface Software Maintenance.....	21
4.10.5.	Interface Software Surveillance	21
4.10.6.	Database Cybersecurity	22
4.10.7.	Database Administration	22
4.10.8.	Unix/Linux System Administration.....	23
4.10.9.	Continuity of Operations (COOP) / Information System Contingency Plan (ISCP)	23
4.10.10.	Dependencies	23
5.	PROGRAM/LIFECYCLE MANAGEMENT.....	24
5.1.	Agile Transition and Support.....	24
5.2.	Requirements/Software Configuration Management Process.....	24
5.2.1.	Information Systems Management Tool (ISMT)	25
5.2.2.	Information Support Request (ISR).....	25
5.2.3.	Historical Workload	26
5.3.	Schedules.....	26
5.3.1.	Schedule Management	26
5.3.2.	Planning Release Roadmap	26
5.3.3.	User Story Management	26
5.3.4.	Product Backlog Management	27
5.4.	Interface Control Documents	27
5.5.	Software and Documentation Control and Release Procedures.....	28
5.5.1.	Software License Management	28
5.6.	Enterprise Software Initiative.....	29
5.7.	Technical Interchange Meetings (TIM) and Technical Reviews	29
5.8.	Monthly Status Report.....	30
5.9.	Deficiency Reports (DRs)	30
5.10.	Software Deployment Planning.....	31
5.10.1.	DMSI and DMCODB Release Support	31
5.10.2.	DMLS Release Support.....	31
5.11.	Maintenance Changes.....	31
5.12.	Software User's Manual (SUM)	32
5.13.	Test Support	32
5.13.1.	Test and Evaluation	32
5.13.2.	Test Readiness Review.....	33
5.13.3.	User Evaluation Testing	33
6.	ENGINEERING REQUIREMENTS	33

6.1. Life-Cycle Systems Engineering.....	33
6.2. Air Force Acquisition Process Model (APM).....	33
6.3. Department of Defense Architectural Framework (DoDAF).....	34
6.4. Standard Desktop Configuration (SDC).....	34
6.5. Cybersecurity Support Personnel	34
7. CONTRACTUAL REQUIREMENTS.....	34
7.1. Place of Performance	34
7.2. Normal Hours of Operation.....	34
7.3. Government Furnished Property.....	35
7.4. Non-Personal Services.....	35
7.5. Contractor Identification	36
7.6. Performance Reporting	36
7.7. Program/Project Management	36
7.8. Services Delivery Summary	36
7.9. Task Management.....	37
7.10. Documentation and Data Management	37
7.11. Records, Files, and Documents.....	37
7.12. Hardware and Maintenance	38
7.13. Section 508 of the Rehabilitation Act	38
7.14. Voluntary Protection Program (VPP) Elements for Requirements Documents	38
7.14.1. Installation-specific Safety and Health Standards.....	38
7.14.2. Applicable Contractors.....	38
7.14.3. Applicable Contractor's Safety and Health Plan	38
7.14.4. Mishap Reporting	39
7.15. Travel.....	39
7.16. Training.....	39
7.16.1. Mission-Unique Training	39
8. SECURITY	40
8.1. Personnel Security Investigation Requirements	40
8.1.1. Security Background Investigation and Clearance	40
8.1.2. Unclassified Contracts.....	40
8.2. Common Access Card (CAC) Issuance and Eligibility	41
8.2.1. CAC Eligibility	41
8.2.2. CAC Requests Submission	41
8.2.3. Interim Issuance of CAC	41
8.2.4. Final CAC Determination	41

8.2.5. Minimum Requirements for Justification	41
8.2.6. Termination, Separation, and Expiration of Contract	41
8.3. Protection of Information	41
8.3.1. Controlled Unclassified Information.....	41
8.3.1.1. Executive Order 13526.....	42
8.3.1.2. Atomic Energy Act of 1954.....	42
8.3.1.3. Specific Program or Project Security Classification Guide.....	42
8.3.2. National Archives and Records Administration CUI Registry.....	42
8.3.3. CUI Guidance	42
8.3.4. Aggregation of Information.....	42
8.3.5. DoDM 5400.07/AFM 33-302.....	42
8.3.6. DoDI 8582.01	42
8.3.7. NIST Special Publication 800-171.....	42
8.3.8. DFARS 252.204-7012	43
8.4. Operations Security	43
8.5. Information Technology (IT) Level Rating.....	43
8.5.1. Critical-Sensitive, Information Technology (IT) Level I positions	43
8.5.2. Non-critical Sensitive, Information Technology (IT) Level II Positions	44
8.5.3. Non-sensitive, Information Technology (IT) Level III positions.....	45
8.5.4. Application & Information System Access Requests	45
8.6. Required Security-Related Training	45
8.6.1. Cyber Awareness Challenge Training.....	45
8.6.2. Force Protection and Anti-Terrorism Training	45
8.6.3. Controlled Unclassified Information Training	45
8.7. In Processing	45
8.7.1. In-Processing Checklist.....	45
8.7.2. Visit Requests for Classified Contracts.....	45
8.7.2.1. Contractors Not Requiring Access to Classified Information.....	46
8.7.2.2. WP Security Office Address.....	46
8.7.3. Visit Requests for Unclassified Contracts.....	46
8.8. Out Processing	46
8.8.1. Out Processing with AFLCMC/GBC	46
8.8.2. Trusted Associate Sponsorship System (TASS)	46
8.8.3. Contractors Ending Association with Air Force/CAC Surrender.....	46

1. INTRODUCTION/PURPOSE

The overall purpose and objective of this effort is to provide maintenance, operations and surveillance support to sustain Depot Maintenance Information Technology (IT) systems by providing software systems analysis, design, sustainment, and maintenance expertise for the system identified within this Performance Work Statement (PWS).

2. SCOPE

This effort is to provide support for the software maintenance, sustainment and surveillance of the Depot Maintenance Systems Integration (DMSI), Depot Maintenance Consolidated Operational Database (DMCODB) and Depot Maintenance Legacy Systems (DMLS). The scope of this effort shall include planning, developing, testing, deploying, and sustaining depot maintenance IT systems to include new development, modifications, enhancements, and upgrades.

3. BACKGROUND

3.1. Depot Maintenance Systems Integration (DMSI)

DMSI is comprised of six (6) applications: AFMC Labor Standards Data System (ALSDS), Depot Maintenance Materiel Support System (DMMSS), Exchangeables Production System (EPS), Inventory Tracking System (ITS), Job Order Production Master System (JOPMS), and Programmed Depot Maintenance Scheduling System (PDMSS). DMSI applications were modernized, technically refreshed, or re-hosted into a consolidated system framework. All DMSI application data were migrated into the Depot Maintenance Consolidated Operational Database (DMCODB), which provides the consolidated database for the production management of the depot repair and maintenance process for the Air Force (AF) Enterprise. DMSI supports approximately 8,000 Headquarters Air Force Materiel Command (HQ AFMC) users at the three (3) Air Logistics Complexes (ALCs) and Kadena Air Base (AB), including inventory management specialists, maintenance specialists, equipment specialists, funds monitors, and quality assurance specialists.

3.1.1. DMSI Client/Server Applications

Only five (5) DMSI client/server applications are within the scope of this PWS:

- 1. AFMC Labor Standards Data System (ALSDS):** Establishes and maintains labor standards for maintenance planning and production costing. It provides information on data used for capacity planning reports that shall evaluate workload and personnel in terms of skills, and a simulation capability in order to determine the impact on skill capabilities and requirements in relation to workload changes.
- 2. Job Order Production Master System (JOPMS):** Provides a repository for storing the production number master records. It also provides the user ability to track customer work requests, record work authorizations, maintain temporary work plans, record end item production, and document standard labor hours earned during depot level maintenance.

3. **Depot Maintenance Materiel Support System (DMMSS):** Acts as a repository for material standards and production/issue history, which supports increased productivity of the Depot Maintenance Work Centers. It provides part number to stock number cross-reference, history of National Stock Number changes, and retrieves, stores and updates Bill of Material (BOM) standard data.
4. **Exchangeables Production System (EPS):** Provides access to workload requirements data, end item availability data, job order number data, production count data, end item production data, on-line information used to manage Depot Maintenance Supply Centers (DMSC) and bench stocks.
5. **Inventory Tracking System (ITS):** Tracks repairable end items through the maintenance overhaul line. It assigns item-tracking numbers to all parts as they are inducted and subsequently tracks them through disassembly, repair, and assembly. The system provides management information to all levels of management as well as inventory control.

3.1.2. Depot Maintenance Consolidated Operational Database (DMCODB)

DMCODB is an integrated, consolidated shared Oracle database that provides data for production management of the Depot repair and maintenance process for the AF Enterprise. It is an operational-level data environment, serving on-line transaction processing applications for managing day-to-day operations in the AF aircraft maintenance depots.

As the depot maintenance applications were modernized, their data was loaded into the DMCODB. DMCODB became a common source of data, receiving their data updates, and sending their data interfaces. It performs application data retrieval and updates, interfaces, and scripts needed to support all system interfaces. Through the DMSI operational applications, the DMCODB supports HQ AFMC users worldwide, including inventory management specialists, maintenance specialists, equipment specialists, funds monitors, and quality assurance specialists. DMCODB also provides corporate-level data to support AFMC tactical and strategic planning activities.

As operational applications are technically refreshed, they are enhanced with new user capabilities for reporting and on-line analytical processing (OLAP). Drawing upon the DMCODB's consolidated data, these systems enable users to extract information, perform analyses, create reports, and respond to information requests from AFMC command-level staff, HQ AF staff, and Department of Defense (DoD) elements. The DMCODB also provides data for Data Services (DS), data marts/warehouses, and Enterprise Integration projects.

3.2. Depot Maintenance Legacy Systems (DMLS)

DMLS consists of two (2) applications used by all three (3) ALCs to perform management, workload forecasting, planning, parts support and tracking and requirements, configuration and workload management. DMLS includes the following systems:

1. **Depot Maintenance Workload Planning and Control System (DMWPCS):** Provides the Depot Maintenance a method to document and track the results of workload and manpower planning actions, provide a planned and historical labor application, interface data to other systems and provide a master listing of all Resource Control Centers (RCC) and their associated accepted workloads factor. The system also provides for multiple

Planned Labor Application (PLA) capability. This system is designed to process in both batch and database environments.

2. **Information System Management Tool (ISMT):** ISMT is the mandated application directed by AFMC/A4 to be used for managing the lifecycle of all application requirements. A portfolio management, requirements management and workload management tracking/reporting tool that supports the entire software lifecycle for Logistics Business IT (LogIT) programs/systems. ISMT is also used to manage the program backlog of tasks that need to be worked within a program release or sustainment cycle.

4. REQUIREMENTS/DESCRIPTION OF SERVICES

4.1. Skills and Knowledge

The Contractor shall have the skills and knowledge necessary to perform requirements and business process analysis, configuration and requirements management, quality assurance, design and construction (coding), software systems engineering, web-based development, documentation development, and testing, implementation and training.

4.1.1. General Skills and Knowledge

The Contractor shall:

- Have proficiency with project management software (e.g., MicroSoft Project, Jira) to create/ deliver integrated schedules
- Have critical technical skills required include using sound program management techniques and processes, expertise in mainframe, cloud, and Web-based environments
- Systematically evaluate, design, and standardize database tables for databases of systems to be subsumed or incorporated into the DMSI or DMLS databases
- Provide software engineering support and technical expertise for defining and analyzing system requirements, developing design specifications, translating specifications into programming logic, coding, completing developmental testing, and additional testing, as required
- Provide support that may include, but is not restricted to, technical leadership to develop solutions for software engineering studies and mainframe, client/server or

Internet/intranet applications, systems engineering, architectural design, structured analysis, and object-oriented principles and tool suites

- Provide software engineering and system analysis to design, develop, test, deploy, document, system restart/recovery, and integrate of new and/or modified information systems
- Provide software engineering evaluation of Commercial-Off-the-Shelf (COTS) software packages for potential integration and use in current/future AFLCMC/GBM depot maintenance software applications
- As required, support subsumption (or consolidation) of application components and capabilities into any future depot maintenance enterprise solution requirements

4.1.2. DMSI Support Skills and Knowledge

The Contractor shall provide the following support skills and knowledge areas:

- ALSDS, DMMSS, EPS, ITS, and JOPMS applications are using client/server architecture with software being deployed by local communication squadrons to the users' workstation.
- DMSI shall be programmed in Oracle Programming Language/Structured Query Language (PL/SQL) and also using Appeon PowerBuilder application development. Procedures to retrieve data and package the business object data calls use SQL Scripts. DMSI implements configuration management using Subversion. InstallShield is used to package the client/server applications for deployment. RoboHelp is used to create the Help files.

4.1.3. DMCODB Support Skills and Knowledge

The Contractor shall provide the following support skills and knowledge areas:

- Knowledge of Oracle 12.x database administration and performance tuning
- Oracle SQL Script
- Oracle PL/SQL
- Oracle GoldenGate, DataGuard, Materialized Views
- Programming Languages: C, Perl, and Extensible Markup Language (XML)
- SubVersion Version Manager
- Information System Management Tool (ISMT)
- IBM Websphere MQ 7.x
- SQL/Net
- FTP/SFTP
- Data Modeling
- UNIX/Linux shell scripting and system administration
- MS Windows Sever Administration
- SmartSVN
- VisualSVN
- Data Modeling and Data Management Tools
 - ERwin v7.x PL/SQL Developer v 8
- Java and JavaScript

4.1.4. DMLS Support Skills and Knowledge

The Contractor shall provide the following support skills and knowledge areas:

- Software maintenance and sustainment support performing mainframe, client/server, internet/intranet and cloud applications; translation of specifications into programming logic, coding, completing developmental and additional testing operations in a Defense Information Systems Agency (DISA) environment. Each DMLS application has its own unique software/ hardware requirement.
- DMWPCS is programmed Azure Cloud Hosted MaaS
 - Mainframe: Microsoft Azure C1
 - OS - Windows Servers 2016
 - DB - Azure SQL Server
 - C#
 - Lines of code: 142,530
- ISMT is a Cloud-based configuration and requirements management application.
 - Cloud Azure PaaS
 - BitBucket
 - Artifactory
 - DB: SQL Server 2018
 - Visual Studio 2019
 - Oracle PL/SQL

- ASP.net
- Code repository – Atlassian BitBucket
- Approx. 855,000 lines of code

4.2. Program Management Plan

The Contractor shall prepare a Program Management Plan describing the approach for conducting and providing analysis, maintenance, testing and surveillance support for this PWS. The Program Management Plan, at a minimum, shall address:

- Staffing Plan, Roles and Responsibilities
- Knowledge Transfer approaches and Internal Training
- Performance Measurement and Critical Success Factors
- Risk Management approach
- Workload Management
- Quality Assurance
- Use of ISMT for Software Configuration Management, including use of other government approved software code management tools
- Software maintenance processes, including documentation update and processing, and management and oversight
- Tools used for monitoring, controlling, and reporting
- Testing as covered in the Integrated Test Plan
- Development and update of project schedules and performance reporting
- Approach and processes for execution of program surveillance activities
- Outbound Transition Plan to Government or future contract resources, including:
 - Approach to be used to train resources
 - Transition of surveillance tasks and responsibilities
 - Transition of maintenance tasks and responsibilities
 - Transition of all source code, documentation, equipment, and support files and plans

4.3. Contractor Responsibilities and Support

The Contractor shall provide sustainment, operations and surveillance support for DMSI client/server applications, DMLS applications, and DMCODB. All systems identified within this PWS have a service level objective of at least 98% availability (i.e., uptime) to the customer. The 98% uptime objective assumes a requirement of continuous uptime (i.e. 24/7 all year long) with allowances for planned maintenance windows. The Contractor shall schedule and coordinate all planned maintenance with the designated Capability Delivery Teams (CDT) and affected stakeholders (i.e. end users, ALCs, DISA, etc.).

The Contractor shall, in cooperation with other DMSI applications and Spectrum System Development Architecture (SSDA) framework, develop DMCODB changes required to meet customer change requests.

The Contractor shall develop and/or modify schedules, coordinate with interfacing systems, and serve as the surveillance Point of Contact (POC). The Contractor shall coordinate special runs and planned system outages with the Office Primary Responsibility (OPR) on schedules, block changes of releases, and special events for both DMLS and DMSI systems. The Contractor shall setup and/or modify site unique system Job Control Language to enhance performance, recovery procedures, and output distribution. The Contractor shall verify successful processing/ completion and/or file status.

The Contractor shall notify the appropriate Program Management Office (PMO) for non-conforming errors, and required restarts/reruns. The Contractor shall detect, analyze, and resolve program or data problems, security violations, process problems and/or conflicts with other system schedules and events. The Contractor shall utilize and update surveillance online documentation to include application help files, as applicable.

The Contractor shall provide the PMO with detailed information concerning program problems. The Contractor shall detect poor and degraded program performance and report this to the PMO. Upon PMO request, the Contractor shall provide Information Support Requests (ISRs), which can be (ad-hoc/out-of-cycle) reports, interrogations, requests and other specified information concerning any aspect of their system. DMSI batch jobs will be addressed, initiated, monitored, coordinated, and implemented through the DMSI PMO.

The Contractor shall provide sustainment and surveillance services to include, at a minimum: software infrastructure, software engineering, technical support, and resolution of priority 1-5 Deficiency Reports (DRs), Software Problem Reports (SPRs), Change Requests (CR), Baseline Change Request (BCRs), Technical Change Requests (TCRs), Software Maintenance (S/W Mx), Code Quality Request (CQR), and Information Support Requests (ISRs) documented in ISMT.

Note:

Refer to Appendix A for DR Severity Code Definitions.

Refer to Appendix B for System Context and Historical Workload Data.

The Contractor shall provide technical editing and writing services in the preparation and maintenance of system lifecycle documents. The Contractor shall establish documentation

guidelines, configuration and version control, procedures and templates, word processing and coordinate final production of deliverables. Development and maintenance of the on-line users' manual shall meet customer standards and requirements.

The Contractor shall execute all phases of software maintenance (as appropriate) using the Department of the Air Force (DAF) Acquisition Process Model (APM).

Additionally, the Contractor shall comply with applicable regulations and standards identified in APPENDIX C. The Contractor shall prepare and submit Technical Solution/Rough Order of Magnitude (TS/ROM) data on all change request types (i.e., S/W Mx, CQR BCR, DR, and TCR) into ISMT, or government designated tracking system.

4.4. Contractor Transition Support

The Contractor shall address their plan to execute the training, transition and turnover of the DMSI client/server applications, DMLS applications, and DMCODB as part of an overall Transition Plan. During the Contract Start-up/Transition, the Contractor shall perform the tasks required for transferring maintenance, sustainment, surveillance and program management support from the incumbent contractor to the new contractor in a collaborative and supportive manner.

4.4.1. Initial Kickoff Meeting

The Contractor shall initiate work on this contract by meeting with AFLCMC/GBM personnel to ensure that a common understanding of requirements, expectations, documentation, and ultimate end products exist between all parties. The Contractor shall then prepare and deliver a Report, Record of Meeting/Minutes.

4.4.2. Contract Start

The Contractor shall submit a non-proprietary Transition Plan covering a 60 day period to include assisting the follow-on contractor in learning all capability support activities (development, surveillance and operations) to ensure minimal downtime. This Transition Plan shall provide for the orderly start-up of maintenance and transfer of all items related to the maintenance of supported systems (i.e., DMSI applications, DMLS applications, and DMCODB), to include, at a minimum: source code, make files and/or other build files, build instructions, use of government approved configuration management tools, application data, application documentation, government furnish property (GFP), and status of work in-process. The Transition Plan shall include a comprehensive description of the activities and schedule required to transition the databases maintenance, sustainment, and technical support functions from the outgoing contractor to the follow-on contractor.

The plan shall include:

- Movement of GFP/Government Furnished Information (GFI), if required
- Resourcing and staffing
- Program Management startup activities

- DMCODB surveillance and operational activities
- Acquiring knowledge and familiarization
- Risk assessment approach/methodology
- Other topics considered necessary for accomplishing a successful transition

The Contractor shall execute their transition plan to:

- Allow no disruption of service to business processes after conclusion of transition
- Accomplish a smooth transfer of daily operations, on-going projects, development and test environments, and other assets
- Ensure qualified personnel, with necessary skills, knowledge and clearances are available at contract award to accomplish a successful transition
- Collaborate and communicate with the Government and the current contractor during the transition period
- Identify and manage any risks associated with the transition, particularly risks associated with human resources and GFP environment transfer, if required
- Complete transition staffing no later than 30 calendar days after contract award

Deliverable: Software Transition Plan (STrP), (CDRL A011)

4.4.3. Contractor 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.

Deliverable: Software Transition Plan (STrP), (CDRL A011)

4.4.4. Transition at Contract Conclusion

The Contractor shall develop a non-proprietary plan for the transition of sustainment, maintenance, operations, and modification responsibilities to the follow-on contractor. The Transition Plan shall provide a plan for the orderly transfer of all items related to the maintenance the DMSI client/server applications, DMLS applications, and DMCODB, to include source code, files and/or other build files, build instructions, configuration management tools and data, database models, documentation, status and documentation of work-in-process, and GFI/GFP, if required, to the follow-on contractor.

The Contractor shall be required to answer functional and technical questions to enable the follow-on contractor to maintain and sustain all applications and interfaces. The follow-on contractor shall have the responsibility to perform these activities, but the incumbent contractor shall continue to provide support to the follow-on contractor during the transition period. The Contractor's transition plan shall include a comprehensive description of the activities and schedule required to transition the maintenance, sustainment, and technical support functions from the outgoing contractor to the follow-on contractor.

The plan shall include transition support for DMSI client/server applications, DMLS applications, and DMCODB:

- Resourcing and staffing
- Program management shut down activities
- DMCODB surveillance and operational activities
- Knowledge sharing and orientation
- Movement of GFP/GFI, if required
- Other topics or activities necessary to accomplish a smooth transition

The Contractor shall execute their transition plan to:

- Allow no disruption of service to business processes
- Accomplish a smooth transfer of daily operations, on-going projects, production, development, test environments, and other assets
- Collaborate and communicate with the Government during the transition period
- Identify and manage any risks associated with the transition particularly risks associated with human resources and GFP environment transfer, if required

Deliverable: Software Transition Plan (STrP), (CDRL A011)

4.4.5. Transition Working Group (TWG)

A TWG shall be established to plan, monitor, and manage the transition of maintenance support from the Contractor. A Government representative will chair the TWG. It will include representatives of the Government Program Management Office (AFLCMC/GBM Depot Maintenance), out-going contractor, functional user, and gaining contractor and/or support contractors. The TWG shall define and coordinate all agreements, actions, events, schedules, training and other requirements needed for an orderly and timely transfer of maintenance and sustainment responsibility from the out-going contractor. The Contractor shall provide status on action items, events, and schedules in minutes from TWG meetings.

Deliverable: Software Transition Plan (STrP), (CDRL A011)

The Contractor shall also be required to meet the Performance Requirements identified in Appendix F: Services Summary.

4.5. Data Analysis

The Contractor shall perform proactive data analysis, recommend corrective actions as a result of analysis, and participate in work groups in support of DMSI client/server applications, DMLS applications, and DMCODB. The Contractor shall perform data analysis and maintain data analysis tools required to research legacy system data for comparison to data in the Data Depot Corporate Model. The Contractor shall provide analysis support for the migration of DMSI, DMLS, and DMCODB data to other Enterprise Integration efforts.

4.6. Enterprise Management Support

The Contractor shall be required to provide support to other AFMC Enterprise initiatives (e.g. MROi, PLMi, etc.) that may materialize as they relate to integration with DMSI, DMLS, and DMCODB. The scope of these efforts may include functional requirements support and analysis, data analysis/integration/support, data modeling, design, development, and interface development/modifications for DMSI client/server applications, DMLS applications, and DMCODB.

4.7. Systems Support

The Contractor shall design, develop, test and package systems and software changes as well as provide problem resolutions for the existing system. The Contractor shall maintain the current baseline of the system and provide software change and problem fixes to these baselines as required. The Contractor shall provide to the Government all developed, modified, or converted programs, scripts, operating instructions documentation, test scripts used to develop each approved systems change request.

Specific tasks may include the following:

- Maintain existing systems and environments in accordance with (IAW) disciplined engineering practices and sustain databases and interfaces in compliance with applicable AF/DoD standards
- Conduct software and data model development, data conversion and data lifecycle management
- Utilize Government-Off-the-Shelf (GOTS) or approved COTS tools for systems design and development

4.8. Development, Test, Training and Production Servers

The Contractor shall also be responsible for performing the following database administration activities specific to DMSI, DMLS, DMCODB development, and test, training, and production servers:

- The Contractor shall set up database structures
- The Contractor shall perform initial database environment configuration for the physical layout of the database environment and storage allocation
- The Contractor shall create or modify database instances; install, upgrade and patch the database software; and adjust authorizations and permissions of users and groups
- The Contractor shall ensure compliance with Security Technical Implementation Guides (STIGs) and Information Assurance Vulnerability Alerts (IAVAs) and perform, maintain and validate Vulnerability Management System (VMS) data entry for all systems and applications identified within the PWS
- The Contractor shall conduct automated Source Code Analysis (SCA) using government approved tools (e.g., such as Checkmarx, Fortify, etc.) on every release/patch that includes new or modified source code
- The Contractor shall provide access to vulnerability assessments within the online tools for each release/patch that includes new or modified source code

- The Contractor also shall conduct cyber security-focused testing (validate on any affected controls/STIGs) and document any flaws found
- The Contractor shall produce/provide results of all security testing and work with the PMO Cybersecurity Team to assess all findings and flaws reported
- The Government cybersecurity team member shall be responsible for confirming the Contractor's assessment of findings that the Contractor determines to be invalid or non-issues. All valid findings identified in the release shall be addressed prior to the code being released into the production environment or at a Government defined date. Valid findings can be addressed through remediation (fix/update code) or through other risk management processes, such the Plan Of Action & Milestones (POA&M) process (STIGs). Furthermore, any remediation decisions shall be documented.
- If Cyber Security incidents are identified in production, the Contractor shall work with the PMO cybersecurity team and other Government personnel from the PMO to prioritize the correction of these incidents. If the vulnerabilities identified are found to be introduced with a release/patch, the Contractor shall be responsible for remediation.
- The Contractor shall schedule and monitor database backups
- The Contractor shall validate the integrity of the database backup process and recovery images annually
- The Contractor shall conduct performance tuning
- The Contractor shall be responsible for release deployment when required

4.9. Agile / Incremental Delivery Methodology

4.9.1. Current Sustainment and Maintenance

The Contractor shall collaborate with the Government to facilitate an Agile-based approach to sustainment support. The prioritization of requirements is subject to change based on Mission Business Area demands during the period of the contract. Planned and forecasted features may be accelerated, changed, or interchanged within the scope as determined in program increment or sprint planning.

The designated Product Owner(s) will specify high-level requirements/capabilities to the Agile Development Team. As in typical Scrum-based agile processes, the Contractor and Product Owner will work together with project stakeholders to develop and estimate user stories and establish acceptance criteria. These acceptance criteria will specify expected functionality for a user story, as well as any non-functional requirements that must be met in the development of the story. The Agency Product Owner, supported by subject matter experts and business analysts, will determine whether or not acceptance criteria have been satisfied.

4.9.2. Surge Requirements

Future surge requirements may be identified throughout the Period of Performance (PoP), such as major technical refresh efforts, which would warrant a contract modification to define surge requirements and exercise the surge CLINs.

As part of this approach, the Contractor shall provide six (6) six-month agile team options that may be exercised per contract year to support increased requirements by the user community (Surge CLINs). These teams shall consist of two developers and one tester. These teams shall be additional to the staffing required to maintain the current requirements in the PWS and shall not be utilized to perform work to be completed under the basic labor CLINs. These increased in-scope

requirements such as new AF or DOD initiatives may include unplanned tasks above/beyond current sustainment and/or maintenance efforts. Examples may include but are not limited to:

- Code refactoring
- Addressing technical debt
- Identity Credentialing Access Management (ICAM) implementation
- Standard Financial Information Structure (SFIS) compliance
- Standard Line of Accounting (SLOA) compliance
- Defense Logistics Management Standards (DMLS) compliance

The Government CO will provide the potential surge requirement to the contractor. The contractor shall then notify the appropriate CDM/PM of the number of surge teams required within 15 business days upon receipt of the requirement. Upon exercise of surge option(s), the surge requirement will be defined within the PWS. When these requirements are exercised utilizing surge labor CLINs, the requirement will be placed into the Contractor's overall product backlog, integrated into the product increment plan, and worked within the programmed release cadence for the agreed period.

4.10. Specific Task Descriptions

4.10.1. Database Integration and Design

The Contractor shall review new and modified database requirements to determine any additions/modifications/clarifications necessary to update the Software Requirements Specifications (SRS) and Database Design Description (DBDD) for each application or database. The Contractor shall develop and integrate data requirements into the data model. The Contractor shall work with the Government PMO, application development teams, SSDA framework and enterprise integration efforts to ensure a satisfactory understanding of the requirements before proceeding with the database design change. The Contractor shall take all actions necessary to resolve any data requirement conflicts with existing data model or proposed changes to the environment. The Contractor shall follow system engineering standards and/or best practices in the development of the logical and physical data models. The Contractor shall review and provide analysis on change requests submitted by developers or Program Office that impact logical and/or physical models. The Contractor shall provide updates to the existing SRS document or United States Government (USG) designated tool.

The Contractor shall monitor development, test, training, and operational environments in coordination with PMO and DISA staff. The Contractor shall perform required activities within the operational environment needed to support database and interface processes. The Contractor shall support the Government in investigating, developing and implementing data or database changes needed to support Air Force Enterprise initiatives.

The Contractor shall evaluate, design, and standardize database tables to be subsumed or incorporated into DMSI, DMLS, or DMCODB. This includes developing and integrating data requirements into the environment.

Deliverable: Database Design Description (DBDD), (CDRL A010)

Deliverable: System Requirements Specification (SRS), (CDRL A005)

4.10.2. Data Conversion

The Contractor shall define data conversion mappings and designs to migrate data from a legacy system environment to support enterprise integration initiatives. The Contractor shall verify data integrity is not compromised and other DMSI, DMLS, and DMCODB are not adversely impacted.

Prior to the start of software testing, the Contractor shall execute data conversion tests using the most current legacy production data. The Contractor shall review the data conversion logs and review the results of the conversion with functional subject matter experts. The Contractor shall identify data that does not conform to the business rules defined in the database design. This dirty data shall be provided to the functional users who shall correct it in the legacy system. The data conversion shall be re-executed to verify the database is ready for testing. During testing, the data conversion shall be performed as required to support the retesting of interface and application software.

4.10.3. Interface Software Design and Maintenance

The Contractor shall implement interface change requests as required by the functional community. The Contractor shall monitor/surveil all interface jobs and batch processes to ensure proper execution. All system interfaces for this PWS are shown in APPENDIX D.

The Contractor shall analyze interface requirements, design interface methods and associated software, and shall demonstrate the current capabilities and status of the design at technical review. The Contractor shall conduct TIMs with software developers and PMO as frequently as necessary to resolve requirements issues, to ensure that the design accurately represent the approved requirements, and are proceeding in accordance with the approved schedule. The Contractor shall verify and maintain the design of interface software with the Interface Control Document (ICD) associated with each interface in the Corporate Data Repository System (CDRS). At the conclusion of the detailed design, the Contractor shall update the Software Design Description (SDD) or Interface Design Description (IDD) artifacts.

The Contractor shall provide an Application Daily Operations Manual (ADOM) to document complete instructions for operating the interface software. This shall include administration functions required for execution and error recovery for the interface.

Deliverable: Software Design Description (SDD), (CDRL A006)

Deliverable: Application Daily Operations Manual (ADOM), (CDRL A012)

4.10.4. Interface Software Maintenance

The Contractor shall provide software maintenance for all interfaces. This software maintenance shall include: attending development team scrum meetings, AF designated governance meetings, and providing analysis on proposed changes/ enhancements/ technical infrastructure changes to the interface software. Changes may be to existing data exchange mechanisms, transformation algorithms, record layouts, or other software modification caused by changes to external systems, database design, and preventative maintenance. Meetings with external systems might be necessary to provide a technical solution. Also, testing with external systems is necessary to ensure the technical solution is correct.

4.10.5. Interface Software Surveillance

The Contractor shall monitor incoming/outgoing interfaces and batch processes to ensure proper execution of all interface software processes. The Contractor is responsible to perform surveillance activities for all DMSI, DMLS, and DMCODB batch jobs. On a daily basis, the nightly batch process logs shall be reviewed to confirm the status of each scheduled interface. The Contractor shall respond 24 x 7 x 365 to interruptions in execution of critical batch processes as identified by the DISA help desk. The Contractor shall coordinate with DISA and cloud support personnel and software developers (DMSI, DMLS, and DMCODB) to implement corrective actions.

The Contractor shall support special job executions and/or other tasks in support of fiscal end-of-year processing. This is a special process that occurs on the night of 30 September through 1 October. These special job executions are coordinated with the site OPRs.

4.10.6. Database Cybersecurity

The Contractor shall perform a cybersecurity review of changes or modifications prior to execution in the production environment. The Contractor shall adhere to applicable DISA Security Technical Implementation Guides (STIGs), Air Force Cybersecurity Program Management, and NIST Cybersecurity Framework and supporting NIST Special Publications. See Appendix C for a list of Technical Standards.

The Contractor shall ensure deliverables comply with, or mitigate risk in cybersecurity control checklists and DISA Application Security & Development STIG.

The Contractor shall perform a cybersecurity review of all changes and follow a software release process for each release. The Contractor shall create default cybersecurity checklists consisting of cybersecurity controls to be answered per release. The Contractor shall complete cybersecurity checklists comprised of cybersecurity controls for each release and shall submit these results as part of the Software Test Report.

Deliverable: Software Test Report (STR), (CDRL A009)

4.10.7. Database Administration

The Contractor shall perform the following database administration activities for the database and application development, test, Software Validation Test (SVT), DMSI Integration Test (DIT), failover, production, and training database instances as specified in the DMCODB Database Instance Listing, APPENDIX E:

- Work with application developers to explain how to interact with the physical database, and how to construct stored procedures and other database objects as necessary
- Create and maintain additional Relational Database Management System (RDBMS) objects, System Select Transactions (SST), System Utility Transactions (SUT) and any required triggers to provide data replication
- Prepare sizing estimates for the physical database and recommend the optimal number and placement of Oracle instances
- Provide support, tool analysis, setup and administration as required in performing the necessary daily administration activities
- Provide on-site training and instruction and design tools as required by the AFLCMC/GBM depot maintenance development personnel. This instruction shall include techniques in integration of various COTS products and the standards and procedures necessary to construct a multiple-site data resource catalog
- Design and implement a physical database from the physical model
- Maintain the logical and physical data model
- Provide database support to other requesting external system for purposes of interface testing
- Perform user account management
- Provide database design, creation, implementation and maintenance support of development and test databases for all application systems

4.10.8. Unix/Linux System Administration

The Contractor shall be responsible for performing Unix/Linux system administration activities via the Service Level Agreement (SLA) with DISA:

- Optimize performance and ensure high availability of Unix/Linux servers
- Proactively monitor system performance and capacity
- Proactively maintain Unix/Linux infrastructure technology to maintain high availability
- Manage, coordinate, test and implement operating system software upgrades, operating system patches and operating system hot fixes on Unix/Linux servers
- Perform fault finding analysis of logged information for reporting of performance exceptions
- Create and maintain scripts to automate system administration tasks
- Perform routine audits of the Unix/Linux operating system and software
- Perform and maintain Unix/Linux operating system software backups
- Install and configure virtualized machines
- Install and configure Unix/Linux operating systems software
- Maintain user account information for the Unix/Linux servers
- Coordinate hardware maintenance activities with DISA representatives
- Identify problems/issues to the appropriate DISA management level to ensure resolution
- Identify risks and appropriate mitigations for Unix/Linux support tasks
- Ensure the Unix/Linux servers comply with Government STIGs and security regulations where appropriate

4.10.9. Continuity of Operations (COOP) / Information System Contingency Plan (ISCP)

- The Contractor shall collaborate with AFLCMC/GBM personnel to establish an ISCP describing coordination and procedures to recover production, development, and training systems quickly and effectively following a service disruption.
- The Contractor shall identify the activities, resources, and procedures to carry out production, development, and training servers processing requirements during prolonged interruptions to normal operations.
- The Contractor shall ensure coordination with personnel responsible for AFLCMC/GBM contingency planning strategies.
- The Contractor shall ensure coordination with DMSI stakeholders and external points of contact (including vendors) associated with execution of ISCP.

4.10.10. Dependencies

DMSI is dependent upon DISA to maintain and operate the hardware and software infrastructure that supports DMSI's web application and database servers. The Contractor shall coordinate with DISA to jointly administer the DMSI failover databases. The database (production), development and test environments are as follows:

- DMSI and DMCODB – 15103 DISA Data Center OKC, Tinker AFB, OK

- DMWPCS – Cloud One Azure MaaS
- ISMT – Cloud One Azure PaaS

DISA DECC Ogden hosts a second DMSI test site and DISA San Antonio (DISA SA) hosts the DMSI failover databases.

- DMWPCS is dependent on C1 Azure
- ISMT is dependent upon Cloud One Azure that supports its application and database.

The Contractor shall coordinate with DISA to jointly administer the development, test, and training databases. The Contractor shall be responsible of coordinating and/or setting up and maintaining the environments for application testing as well as testing external interfaces. The Contractor shall be responsible for supporting and coordinating schedule and/or out-of-cycle maintenance outages as applicable with DISA, Cloud One, site users, and other impacted teams (DMSI, DMLS, etc.). Technical refreshes of the environments are part of the DISA or Cloud One Service Level Agreements (SLAs). The Contractor shall provide test and integration support to DISA for the DMSI systems and databases.

5. PROGRAM/LIFECYCLE MANAGEMENT

5.1. Agile Transition and Support

AFLCMC/GB4 has identified implementation and maturity of Agile processes and practices across all product lines as critical to achieving its organizational objective for system-wide modernization. As this is an ongoing organizational objective, the Contractor shall support and participate in the implementation of Agile processes in the execution of sustainment and surveillance services. The Contractor shall use the government designated tools in the electronic delivery and reporting of information.

5.2. Requirements/Software Configuration Management Process

The Contractor shall comply with configuration management policy, for all development and sustainment program/projects. The Contractor shall participate in all Functional Review Boards (FRBs) activities as scheduled and provide support to all Software Configuration Control Board (CCB) and Sprint Planning activities.

The Contractor shall use tools approved by AFLCMC/GBM Depot Maintenance for all applicable software configuration, data management, and requirements traceability. The Contractor shall provide configuration identification and change control tasks associated with the receipt, processing, approval and filing of system requirements, design and test documents; in conjunction with the applicable CR method. The Contractor shall capture Functional Description Data (FDD), where the FDD specifies the functional decomposition, and associated requirements, to translate

stakeholder user stories to use-cases (functional and non-functional). These requirements shall not be acted upon/accepted by the Contractor until the Government officially approves them.

5.2.1. Information Systems Management Tool (ISMT)

The Contractor shall use ISMT to manage and track all change requests (i.e., S/W Mx, CQR, DR, SPR, BCR, TCR, and CR) identified by the user community and/or any other tool approved by the Government. The Contractor shall perform analysis and planning for tasks approved for work.

A Technical Change Request (TCR) is a technical requirement performed under sustainment for the purposes of making required operational environment changes or updates to keep the hardware system/environment operational (e.g. server upgrades, COTS version upgrades, etc.). TCRs are attached to a CR (CR acts as a carrier in ISMT for workload routing purposes). A TCR can also be generated to accomplish technical software changes that do not change the functionality of the application but changes the technical approach used. For example, changing code to improve run-time performance of a specific function, changing a device usage characteristic, or changing a process to accomplish the same result such as the use of a different COTS product.

All requirements and change requests (i.e., BCR, CQR, TCR and DR) are entered into the Problem Tracking System module of ISMT by either the user/functional community or the PMO. Upon receiving ISMT notification or PMO direction, the Contractor shall enter Technical Solution – Rough Order of Magnitude (TS-ROM) information into ISMT for each requirement (BCR, CQRs, TCR and/or DR) within 15 work days of the request/notification. The TS-ROM will include a description of the proposed technical solution and estimated labor hours required. The TS-ROM is used by the AFMC governance approval process in determining the overall effort/scope needed for a given requirement.

The Contractor shall maintain all source and executable code. The Contractor shall create and manage project software baseline libraries. The Contractor shall manage requirements and track the status in ISMT of each requirement from the time it is received through release. The Contractor shall update software baselines to production sites. The Contractor shall perform periodic and scheduled audits of the software baselines to verify and document their accuracy. The Contractor shall define and maintain library and file naming conventions. The Contractor shall establish and maintain the functional baselines in the form of a SRS, as well as other documentation as requested by the PMO. The Contractor shall maintain the software development libraries to facilitate the development, test and implementation of software.

Deliverables: Software Version Description (SVD), (CDRL A004)

Deliverables: Systems Requirements Specification (SRS), (CDRL A005)

Deliverables: Source Code, (CDRL A015)

5.2.2. Information Support Request (ISR)

An ISR documents any workload that is used to document, track and manage any requested workload that is not covered by CR, DR, SPR or normal system surveillance.

Examples for use of an ISR are those requested tasking from the PMO, customer or ALCs that comprise, at a minimum:

- Investigate Root Cause
- Generation of one time reports
- Trouble shooting activities
- Production preparation workload
- Database administrator tasks to support developing organizations
- Standard Desktop Configuration (SDC) pre-release testing, and/or
- Assisting with general external system interface questions and/or meeting participation

5.2.3. Historical Workload

The actual number of BCRs, CQRs, DRs, TCRs, SPRs, and ISRs will vary due to the complexity of the changes, customer requirements, prioritization, budget, and external policy direction. Appendix B: System Context and Historical Workload Data, provides a historical workload data for DMSI, DMLS, and DMCODB programs since 2016. The historical workload data reports the total number of releases per year. ISRs are worked as they occur and are not tied to system releases.

5.3. Schedules

The Contractor shall provide inputs to all Government-designated scheduling tools and artifacts supporting DMSI, DMCODB and DMLS for all work identified in the PWS. The schedule shall be constructed for the timely achievement of milestones designated by the Government, shall reflect a logical and executable sequence of effort, and shall be maintained via an approved Government maintained baseline. The Contractor shall ensure time-phased work plans corresponds to the baseline schedule. Detail schedules used for workload tracking shall be provided to the Government upon request. Baselines shall not be changed without prior Government PMO authorization.

5.3.1. Schedule Management

AFLCMC/GB has adopted agile software methodologies for incremental sustainment of LogIT systems. The Contractor shall coordinate with the Government in defining a common, non-proprietary, approach to define and maintain a schedule for all work identified in the PWS. The schedule shall extend to a sufficient level of detail to mitigate risk and measure performance, and shall ensure vertical and horizontal traceability is maintained at all times.

5.3.2. Planning Release Roadmap

The Product Roadmap (PR) shows the strategy used to drive the priorities in the Product Backlog. The Contractor shall prepare a PR for the estimated schedule of when product features will be released. The PR is the foundation for the agile project schedule. The Contractor shall prioritize development in accordance with the Product Backlog.

5.3.3. User Story Management

Prior to executing any work, the Contractor shall develop (in conjunction with stakeholders) a user story and obtain approval. It is assumed the creation of stories will require participation from multiple stakeholders (Business Units, etc.). The Contractor shall be responsible for the coordination of all activities required to complete each story. The Contractor shall be responsible

for tracking and decomposing each story down to the working level or sprint (generally requiring less than 10 business days to complete the story). The Contractor shall clearly show traceability and dependencies between stories. At the request of the COR, the Contractor shall develop milestones and a detailed schedule for more complex stories.

5.3.4. Product Backlog Management

The Product Backlog contains the complete set of prioritized Epics, Features, and User Stories with bi-directional traceability to the program requirements and highlights known work yet to be completed. The Contractor shall work closely with the Government designated Product Owner/Product Team to ensure that the Product Backlog is continually and regularly maintained in alignment with the Agile cadence so that the necessary Release and Sprint Backlog items (epics, features, and user stories) are defined with acceptance criteria and prioritized by the designated Representative/Product Owner/Product Team prior to the start of each release and sprint.

The Government designated Representative/Product Owner will provide guidance on activities for each planned release for inclusion in the schedule (as required by release). The Contractor shall collaborate with stakeholders to refine (i.e., groom) the Product Backlog, Product Release Plan, and develop user-stories. Examples of collaborative reviews and milestones include the following:

- Product Increment Planning (Requirements, Design, and Build and Test activities for each release)
- Sprint Reviews (that may include incremental engineering reviews, such as Systems Requirement Review (SRR), Preliminary Design Review (PDR), Critical Design Review (CDR) and Test Readiness Review (TRR))
- Qualification Test & Evaluation (QT&E)
- Full Deployment Decision (FDD)
- Release to Production/Full Operational Capability (FOC)
- Working groups and Integrated Product Teams (IPTs) that contend with production problems; troubleshooting production errors, performance problems, installation issues, and cybersecurity issues

Deliverable: Program Schedule/Agile Release Plan and Roadmap, (CDRL A002)

Deliverable: Program Release Package, (CDRL A003)

5.4. Interface Control Documents

The Contractor shall participate in the development, revision, coordination, and maintenance of Interface Control Documents (ICDs) related to the appropriate system(s). If sustainment tasks on this effort require the Contractor to create or modify an ICD, the Contractor shall be responsible for preparing the new or revised ICDs using the Corporate Data Repository System (CDRS).

The Contractor shall develop and unit test the interface methods and associated software to meet the combined interface requirements of system enhancements/modification efforts identified by the Government for incorporation into the respective environments.

DMLS and DMCODB interfaces are identified in APPENDIX D.

5.5. Software and Documentation Control and Release Procedures

The Contractor shall maintain software development libraries to facilitate development, test and implementation of DMSI, DMLS, and DMCODB interface software. System documentation shall be on-line to the maximum extent practical. The Contractor shall update SDDs associated with requirement changes in the SRSs. The Contractor shall provide the Government a Software Version Description (SVD) for the entire deployment package (source code, executables and load procedures) and all final system documentation in compliance with the AF APM.

For each version release that results from updates, modifications and/or defect fixes of the operational system, the following documents (as required by the PMO), and any additional documents requested by the Program Manager and are to be delivered electronically to the Contracting Officer Representative (COR) and Capability Delivery Manager (CDM) prior to implementation of a release.

Deliverable: Program Release Package, (CDRL A003)
Deliverable: Software Version Document (SVD), (CDRL A004)
Deliverable: System Requirements Specification (SRS), (CDRL A005)
Deliverable: Software Design Description (SDD), (CDRL A006)
Deliverable: Software Test Plan (STP), (CDRL A007)
Deliverable: Software Test Descriptions (STD), (CDRL A008)
Deliverable: Software Test Report (STR), (CDRL A009)
Deliverable: Database Design Description (DBDD), (CDRL A010)
Deliverable: Software User's Manual (SUM), (CDRL A013)
Deliverable: Software Development Plan (SDP), (CDRL A014)
Deliverable: Source Code, (CDRL A015)
Deliverable: Requirements Traceability Matrix (RTM), (CDRL A016)

5.5.1. Software License Management

If developing and/or sustaining a system that requires and/or contains COTS, the Contractor shall provide maintenance and support of that software license to manage its relationship to the overall system life-cycle, which would include applications, license agreements, and software upgrades. COTS patches are typically initiated by an ISR to determine system impacts which can potentially result in a TCR, S/W Mx, or CQR change.

The Contractor shall provide asset inventory and services that track the financial aspects of an asset to include cost and depreciation, contract management, leases, maintenance agreements and service contracts. The Contractor shall provide support summary information to include the general terms and conditions, benefits, strategic and tactical directions, license ordering information, internal billing process, pricing and deployment and support of the products included in the agreement. The Contractor shall support common practices for ordering assets, tracking orders and assets, and tagging the assets. The Contractor shall support application installation, operations, customer support, training, maintenance, and sustainment and configuration control, to include the procurement of supporting software licenses.

Deliverable: Software Version Description (SVD), (CDRL A004)
Deliverable: System Requirements Specification (SRS), (CDRL A005)

Deliverable: Software Design Description (SDD), (CDRL A006)
Deliverable: Software Test Descriptions (STD), (CDRL A008)
Deliverable: Software Test Report (STR), (CDRL A009)

5.6. Enterprise Software Initiative

In situations where the purchase of new COTS software is needed to satisfy the requirements of a particular contract, the Contractor shall use available existing enterprise licenses. If enterprise licenses are unavailable, then products will be obtained via the DoD Enterprise Software Initiative (ESI) Blanket Purchase Agreements (BPAs). If products are unavailable from ESI, then products will be acquired through the contractor's ODC CLIN contract. The updated listing of COTS software available from DoD ESI sources can be viewed on the web at <http://www.esi.mil>. All software purchased shall be on the Air Force Evaluated Product List (EPL) if the software operates in a Government environment. If licenses are needed that aren't on the list, it is the contractor's responsibility to get on the EPL.

Deliverable: Software Version Description (SVD), (CDRL A004)
Deliverable: System Requirements Specification (SRS), (CDRL A005)
Deliverable: Software Design Description (SDD), (CDRL A006)
Deliverable: Software Test Descriptions (STD), (CDRL A008)
Deliverable: Software Test Report (STR), (CDRL A009)

5.7. Technical Interchange Meetings (TIM) and Technical Reviews

The Contractor shall participate in TIMs with the Government. TIMs shall be combined with other reviews whenever possible. TIMs can be convened by either the Contractor or Government. The TIM can be face-to-face or virtual.

The Contractor shall conduct the following technical reviews with the Government:

- Preliminary Design Review (PDR)
- Critical Design Review (CDR)

The Contractor shall support the following reviews with the Government:

- Test Readiness Review (TRR)
- Full Deployment Decision (FDD)

The Contractor shall support and provide artifacts/documents for AF APM reviews (i.e. PDR data package) two (2) workdays prior to the review. The Government reserves the right to conduct other types of reviews when deemed necessary.

Deliverable: Program Release Package, (CDRL A003)

5.8. Monthly Status Report

The Contractor shall provide a Monthly Status Report (MSR), delivered on the 10th day of the month, covering the previous month. The MSR shall cover the general health of all sustainment and related initiatives on a monthly basis. The MSR shall include comprehensive status of scheduled release work, inclusive of CRs, BCRs, TCRs, DRs, ISRs, and SPRs. The Contractor shall use the government designated tools in the electronic delivery and reporting of information.

Developmental metrics for each active release, to include:

- Requirements stability (change over system/sub-system baseline, stability within release)
- Product quality
- Interface development status
- Current project risks and issues, including risk mitigation plans and issue contingency plans
- Work planned or scheduled for the ensuing month(s) which can be represented within the Backlog and Sprint Plan
- Project resource levels and explanation of resource changes
- Status of all assigned action items
- Status of contractor's monitoring of quality assurance, configuration management, and security management
- Status of any identified process improvement activities
- Status of deliverables, including required delivery dates and the dates the products are actually delivered
- Summary description of travel and/or other services provided during the reporting period, not described elsewhere in the report
- Annotate and notify the government of any additional issues that may impact the project

The Contractor shall develop a metric performance baseline against the agreed upon metrics on which the actual performance shall be compared. All metric performance baselines shall be subject to PMO approval, and, once approved, shall not be changed without prior PMO approval. The Contractor shall present and discuss the status of performance metrics.

Deliverable: Monthly Status Report, (CDRL A001)

5.9. Deficiency Reports (DRs)

When the Program Office receives a DR requesting a TS/ROM, the Government will task the contractor to accomplish the activities detailed below:

- The Contractor shall provide an analysis translating the deficiency into a detailed TS/ROM. This solution needs to include all screens and On-line Help manuals.
- The Contractor shall include all database changes (DBCRs), JCL changes, and all other changes needed to accomplish the requirement.
- Identify and discuss any programmatic risk related to the completion of the DR. For each risk, describe the mitigation strategy, how it will be accomplished and how it will be reported.

- The Contractor shall provide a Rough Order of Magnitude (ROM) estimate, with supporting rationale, reflecting the level of effort required to complete the DR.
- The Contractor shall develop a preliminary schedule detailing the activities and milestones required to complete the DR. The solution work schedule, at a minimum, shall include milestones for and activities related to PDR, CDR, and TRR.

Deliverable: Program Schedule/Agile Release Plan and Roadmap, (CDRL A002)

5.10. Software Deployment Planning

The Contractor shall coordinate with the software developers, perform planning, and support the development of an implementation checklist to ensure an efficient and effective sustainment of all application and database updates (i.e., DMSI, DMLS, and DMCODB). A Full Deployment Decision (FDD) shall be supported to ensure that all implementation plans, database conversions/loads, testing results, and documentation are in place before interface and data conversion software deployment begins. The Contractor shall schedule, coordinate and support monthly maintenance outages with DISA and cloud enclaves.

The Contractor shall install all applications, supporting database and interface software in accordance with the approved Software Installation Plan (SIP). The Contractor shall be required to occasionally work outside normal business hours to support software releases, DISA's/cloud planned maintenance outage, and unscheduled outages. The Contractor shall support the implementation sites during the production cutover period. The Contractor shall migrate interface and data conversion software to the production environment in accordance with the implementation checklist. The Contractor shall deliver a Software Deployment Package which includes software code.

5.10.1. DMSI and DMCODB Release Support

- DMSI is expected to have from four (4) to six (6) releases annually.
- DMCODB is expected to have from four (4) to six (6) releases annually.

5.10.2. DMLS Release Support

- DLMS will have on average two (2) releases per year for ISMT and DMWPCS will have releases as needed.

Deliverable: Program Release Package, (CDRL A003)

5.11. Maintenance Changes

A prioritized task listing which represents the current maintenance changes in the order of priority shall be provided to the Contractor as deemed necessary for each system. The Contractor shall maintain this prioritized task listing and it shall be reviewed with the Government at each Status Review. After approval of added and/or deleted tasking, as well as changes in priority of existing tasks, a new prioritized listing shall be forwarded to the Contractor. As new requirements are finalized and prioritized, a TS/ROM shall be requested.

The Contract shall develop a preliminary schedule detailing the activities and milestones required to complete the delivery. The schedule, at a minimum, shall include milestones for and activities related to PDR, CDR, and TRR.

5.12. Software User's Manual (SUM)

The Contractor shall maintain and deliver a system-specific Software User's Manual, as required. The SUM shall be available on-line and shall be used to develop help features implemented IAW the latest version of the "User Interface Specification for the Defense Information Infrastructure (DII), Chapter 11."

Deliverable: Software User's Manual (SUM) (CDRL A013)

5.13. Test Support

5.13.1. Test and Evaluation

The Contractor shall assist in the planning, research, preparation, development (to include automated test scripts), execution, and evaluation of test cases (and scripts) and coordination during these phases with the PMO.

The Contractor shall maintain a Software Test Plan (STP) and supporting Requirements Traceability Verification Matrix (RTVM). The RTVM provides bidirectional traceability from high-level system performance requirements to the lowest-level requirements. The STP shall be sufficiently definitive to enable the PMO to assess the adequacy of the test planning. In some testing, test scripts might be needed to setup certain scenarios to be tested. These scripts would be covered in the Software Test Description (STD).

The Contractor shall generate and document Software Problem Reports (SPRs) in ISMT. The Contractor shall be responsible for adhering to the test requirements and test group coordination of the AFLCMC/GBM Depot Maintenance Systems Section, Wright-Patterson (WPAFB). The Contractor shall provide Independent Test Support. The Independent Test Team (ITT) coordinates with the developer throughout the software project to ensure that thorough tests shall be conducted to verify that the system satisfies its functional and operational requirements. The contractor shall prepare Software Test Plan (STP), Software Test Description (STD), and Software Test Reports (STR) as required, and coordinate them with the PMO.

The Contractor shall assist in User/Customer Acceptance testing (Quality Test & Evaluation (QT&E)) of the interface software concurrent with the same type of testing for application software. The Contractor shall work with the software development teams to coordinate the execution of tests at each stage and consolidate results of the tests. The results of the tests shall be assessed by the Contractor prior to releasing the interface software for the next successive stage of testing. The Government will assess test results from User/Customer Acceptance testing. The Contractor shall assist the test team in the performance of interface testing by providing technical support for the setup and execution of the tests. During all test stages, the Contractor shall rework and redeliver software and database structures to resolve Software Problem Reports (SPRs).

5.13.2. Test Readiness Review

The Contractor shall support DMSI, DMLS, DCMODB and HQ test teams in conducting any TRR at the conclusion of test phases. The Contractor shall support a TRR after Component Validation and Integration (CV&I) testing is completed and prior to formal Government validation/acceptance testing. Also, a Software Test Report (STR) shall be produced to summarize the results conducted prior to the TRR. The Contractor shall also provide technical collaboration and support testing activities where applications interface with systems (internal and external), depending on changes to existing system interfaces or addition of new interfaces.

5.13.3. User Evaluation Testing

Prior to deployment to production, the ALCs will commence to test the products in actual field conditions in a test environment, called User Evaluation Testing (UET). As directed by the Government, the Contractor shall correct SPRs and provide technical support to the Government acceptance test team.

Deliverable: Program Release Package, (CDRL A003)

Deliverable: Software Test Plan (STP), (CDRL A007)

Deliverable: Software Test Description (STD), (CDRL A008)

Deliverable: Software Test Report (STR), (CDRL A009)

Deliverable: Requirements Traceability Matrix (RTM), (CDRL A016)

6. ENGINEERING REQUIREMENTS

6.1. Life-Cycle Systems Engineering

The Contractor shall employ disciplined systems engineering processes including, at a minimum, 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 in accordance with Air Force Instruction (AFI) 63-101/20-101, Integrated Life Cycle Management.

6.2. Air Force Acquisition Process Model (APM)

The Contractor shall follow and refer to the AF APM website for common plans, procedures, checklists, forms, and templates that support system life cycle management and systems engineering processes, or be able to demonstrate comparable Capability Maturity Model Integrated (CMMI) processes and artifacts. The Contractor shall also be expected to perform work in an Agile Software environment. This means supporting applications as they establish a sprint cadence in deploying changes on a defined schedule.

The Contractor shall develop solutions that employ principles of open technology development and a modular open systems architecture for hardware and software as described in the DoD Open Technology Development Guidebook. The Contractor shall ensure appropriate data sharing and discovery IAW Department of Defense Instruction (DoDI) 8320.02.

6.3. Department of Defense Architectural Framework (DoDAF)

The Contractor shall support the Government or Government contractor in the preparation of supporting architectural documentation in compliance with the latest Department of Defense Architectural Framework (DoDAF) Enterprise Architecture (EA) guidance version 2.02 established in August 2010.

6.4. Standard Desktop Configuration (SDC)

All services provided under this contract shall function and be in compliance with the SDC.

6.5. Cybersecurity Support Personnel

Personnel performing cybersecurity support activities are required to obtain, and remain current with, technical and/or management certifications to ensure compliance with the latest version of DoD 8570.01-M, Information Assurance Workforce Improvement Program.

7. CONTRACTUAL REQUIREMENTS

7.1. Place of Performance

Work shall be performed at the Government or alternate work location, as approved by the Government, provided appropriate equipment is present at the alternate work location to meet the terms and conditions of the contract and PWS. The Contractor may permit employees to work at an alternate duty location provided prior Government notification is coordinated and the terms of the contract and PWS continue to be met.

The Contractor Program Manager for DMAC-2 shall be located full-time at WPAFB. Workspace will be comparable to that provided to other Government personnel performing comparable or like jobs. The Government will provide the Contractor access to meeting rooms and other facilities as necessary to complete the work described. Any deviation from the determined location requires prior approval of the CO.

7.2. Normal Hours of Operation

The Contractor personnel shall perform their work between the hours of 0600 to 1800 Eastern Standard Time (EST), Monday through Friday, excluding the following Government-observed holidays:

New Year's Day

President's Day

Juneteenth

Labor Day

Veteran's Day

Christmas Day

Martin Luther King Day

Memorial Day

Independence Day

Columbus Day

Thanksgiving Day

Check the Office of Personnel Management (OPM) website for the complete list of Government-observed holidays. In addition to the days designated as holidays, the Government observes the following days:

Any other day designated by Federal Statute
Any other day designated by Executive Order
Any other day designated by the President's proclamation

On Government-observed holidays and days designated by Federal Statute, Executive Order, President's proclamation, or base closure due to inclement weather, the contractor personnel may be permitted to work outside of normal work hours from an alternate work location provided prior Government notification and approval is coordinated and appropriate equipment is present at the alternate work location to meet the terms and conditions of the contract and PWS.

The Contractor shall be required to occasionally work outside normal working hours to support software releases, DISA's/cloud planned maintenance outage, or unplanned system outages.

The Contractor personnel may be permitted to work outside of normal work hours while on base without prior approval or authorization by CO or COR provided it is coordinated with the Program Lead.

7.3. Government Furnished Property

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

- Windows PC with Microsoft Office Suite (Outlook, Word, Excel, PowerPoint, etc.)
- Telephone (local/long distance calls authorized as dictated by contractor performance requirements)
- Copier
- Printer

Copies of required Government furnished materials cited in the solicitation, PWS, and/or in the contract 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 contract's period of performance.

7.4. 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. Pursuant to Federal Acquisition Regulation (FAR) 37.104, Personal Services Contracts, personal services are prohibited unless authorized by statute. 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 contract CO as soon as possible, but no later than within 24 hours. 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.

7.5. Contractor Identification

All contractor/subcontractor personnel shall be required to wear AF-approved or provided picture identification badges so as to distinguish themselves from Government employees. Contractor shall not assign foreign nationals to work any part of this contract. The Contractor shall maintain a roster to identify all contractor personnel assigned to the contract. 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.

7.6. Performance Reporting

The Contractor's performance will be monitored by the Government and reported annually in the Contractor Performance Assessment Reporting System (CPARS) IAW AF AFI AFMC 64-107, *Contractor Performance Assessment Reporting System (CPARS)*. Performance standards shall include the contractor's ability to provide or satisfy the following:

- Provide quality products and customer support
- Timely and accurate reports
- Responsive proposals

7.7. Program/Project Management

The Contractor shall identify a Lead Program/Project Manager (PM) who shall be the primary representative responsible for all work awarded under this contract, participating in program/project reviews and ensuring all standards referenced herein are adhered to. The Lead PM is a key position (or positions), and is critical to the contractor team. The Contractor shall notify the CO and applicable program office regarding changes with the identified Lead PM. The Lead PM is defined as the individual who shall lead a team of professionals to successfully execute this contract. The Lead PM shall exercise authority for planning, executing, directing, coordinating, and administering multiple tasks which can be routine or complex across multiple program offices and geographically separated locations.

7.8. Services Delivery Summary

Reference Appendix F, *Services Summary*, of this PWS for specific performance objectives.

7.9. Task Management

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

7.10. Documentation and Data Management

The Contractor shall establish, maintain, and administer an integrated data management system for collection, control, publishing, and delivery of all program documents. The data management system shall include, at a minimum, the following types of documents: CDRLs, white papers, and status reports. The Contractor shall provide the Government with electronic access to this data, including access to printable reports. All products resulting from this contract shall be the property of the Government with unlimited rights.

7.11. 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. This may include access to Controlled Unclassified Information (CUI) and technical information as defined in Defense Federal Acquisition Regulation Supplement (DFARS) Clause 252.204-7012, *Safeguarding Covered Defense Information and Cyber Incident Reporting*. Use this instruction with DoD 5220.22-R, *Industrial Security Regulation*; DoD 5220.22-M, *National Industrial Security Program: Procedures for Government Activities Relating to Foreign Ownership, Control, or Influence (FOCI)*, Volume 3; and DoD 5200.01-M, V1-4, *DoD Information Security Program*; and if necessary, DoD 5220.22-M, *National Industrial Security Program Operating Manual (NISPOM)*, IAW AFI 16-1406, *Air Force Industrial Security Program*. 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).

7.12. Hardware and Maintenance

The Contractor shall acquire, install, maintain, and provide hardware products and hardware maintenance required to accomplish DMSI, DMLS, and DMCODB PWS tasks. At the termination or completion of the contract, all items purchased with Government funds shall become the property of the Government. The Contractor shall obtain CO approval prior to the purchase of any hardware.

7.13. Section 508 of the Rehabilitation Act

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.

DMSI has been granted a permanent exemption of Section 508 requirements due to DMSI being exclusively used in a maintenance environment.

7.14. Voluntary Protection Program (VPP) Elements for Requirements Documents

VPP is an Occupational Safety and Health Act Program which reflects Congress' intent "to assure so far as possible every working man and woman in the Nation has safe and healthful working conditions and to preserve our human resources by encouraging employers and employees in their efforts to reduce the number of occupational safety and health hazards at their places of employment, and to stimulate employers and employees to institute new and to perfect existing programs for providing safe and healthful working conditions."

7.14.1. Installation-specific Safety and Health Standards

Wright-Patterson AFB is in the process of pursuing VPP recognition or has been recognized under the Occupational Safety and Health Act (OSHA) Voluntary Protection Program (VPP). VPP impacts all — applicable contractors operating on AF installations. It is the contractor's responsibility to ensure its employees and managers have a comprehensive understanding of VPP as well as full compliance with OSHA requirements. The Contractor shall follow the safety and health rules of the installation or VPP site. Detailed information on VPP is available on the OSHA website at <https://www.osha.gov/dcsp/vpp/index.html>.

7.14.2. Applicable Contractors

These requirements apply only to contractors whose employees work more than 1000 hours per quarter. The Contractor shall flow down these requirements to all subcontractors who qualify as applicable contractors under this contract.

7.14.3. Applicable Contractor's Safety and Health Plan

Each applicable contractor shall submit its safety and health plan and corresponding site safety checklist to the contracting officer 10 days after contract award. The safety office will assist the contracting officer to ensure that the contractor's safety and health plan includes all required

elements identified in the PWS. The Contractor's plan shall include appropriate measures to ensure the contractor reacts promptly to investigate, correct and track alleged safety & health violations and/or uncontrolled hazards in contractor work areas. It is the contractor's sole responsibility for compliance with OSHA (Public Law 91-596).

7.14.4. Mishap Reporting

An applicable contractor shall ensure its employees and subcontractors promptly report pertinent facts regarding mishaps involving reportable damage or injury to the AFLCMC/GB AF Security [http://AFLCMC.HI.WPSecurity@us.af.mil](mailto:AFSecurity@us.af.mil) and cooperate (IAW AFI 91-204) in any AF safety investigation. Cooperation will include toxicology testing.

7.15. Travel

The Contractor shall coordinate specific travel arrangements with the individual CO or COR to obtain advance, written approval for the travel about to be conducted. The Contractor's written request shall contain the dates, locations, and estimated costs of travel. If any travel arrangements cause additional costs to the contract that exceed those previously negotiated, written approval by the CO is required, prior to undertaking such travel. Costs associated with contractor travel shall be IAW 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 the tourist class, economy class, or similar accommodations to the extent they are available and commensurate with mission requirements. The Contractor shall provide complete documentation with each invoice supporting the travel costs, to include copies of receipts for all transportation, including air fare, rental cars, parking, hotel accommodations, business-related phone calls, taxi fares, and gasoline. Travel will be reimbursed on a cost reimbursable basis; no profit or fee will be paid. Travel does not include vicinity travel within a 50-mile radius of the designated work location.

7.16. Training

Contractor personnel are required to possess 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 or reimbursable as Other Direct Cost (ODC).

7.16.1. Mission-Unique Training

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

reimbursed by the Government are mission essential and in direct support of unique or special requirements to support the billing of such costs against the TO.

The Contractor shall provide Operation Security (OPSEC), Communications Security (COMSEC) and Cybersecurity (CS) training as part of its overall training requirements. OPSEC, COMSEC, and CS training outline specific actions to protect classified and sensitive unclassified information, activities, and operations during the course of the contract. Critical Information (CI) may apply to tasks associated with this contract and, when applicable, must be protected to prevent adversary collection and exploitation.

The Contractor shall implement security requirements as listed in the OPSEC Plan, which will be provided by the Government. Visitor group personnel shall participate in the Government activity's initial and recurring security training IAW AFI 16-1404, *Air Force Information Security Program Management*; AFI 16-1406 v2, *Air Force National Industrial Security Program: Industrial Security Procedures for Government Activities*, AFI 10-701, *Operations Security (OPSEC)*, and the *Visitor Group Security Agreement*, Training Section.

8. SECURITY

In accordance with DOD Manual 5200.01 DOD Information Security Program, all systems, data, and services identified within this PWS are determined as unclassified.

8.1. Personnel Security Investigation Requirements

Contractors shall submit to the CO and Government PM a list of personnel who require a Common Access Card (CAC) and Government-Furnished Equipment. The Contractor shall identify each person by full legal name, their proposed assigned position, duty location, security clearance required by the contract, the company for which they work, full contract number (including task order, if applicable), and the contract end date. The Prime Contractor shall include the information for all subcontractors. If applicable, the personnel list shall also identify persons who need Secret Internet Protocol Router Network (SIPRNET) and/or privileged access. For privileged access, the list shall explicitly specify which IT Level – I or II – is needed.

8.1.1. Security Background Investigation and Clearance

Contractor personnel shall have the appropriate security background investigation or security clearance (i.e. eligibility) prior to the performance of duties in support of this contract.

8.1.2. Unclassified Contracts

For unclassified contracts, the Contractor shall have at least a favorably adjudicated Tier 1 (T1) investigation or its equivalent, the National Agency Check with Written Inquiries (NACI). If a favorable T1 or NACI is not indicated in the Defense Information System for Security (DISS), the prime contract may request, through the government program manager, that a T1 investigation be initiated.

8.2. Common Access Card (CAC) Issuance and Eligibility

8.2.1. CAC Eligibility

IAW DoDI 5200.46, DoD Investigative and *Adjudicative Guidance for Issuing the Common Access Card*, Enclosure 4, Paragraph 3, Application of the Standards; DoDI 5200.02, *Personnel Security Program*; Homeland Security Presidential Directive (HSPD)-12; and AFMC Guidance for the Credentialing of Un-cleared Contractors, dated 13 November 2018, Attachment, Paragraph 5a, eligible contractor personnel requiring physical access to a DoD or AF facility or installation as their normal work location; the Air Force Network (AFNet); a DoD Automated Information System (AIS); Controlled Unclassified Information (CUI), or any equipment not involving access to classified information shall obtain Common Access Cards (CAC).

8.2.2. CAC Requests Submission

The PM, COR, or other government person associated with the program shall submit contractor CAC requests to the security office that services that program. For programs administered by AFLCMC/GB offices on Wright-Patterson AFB, submit CAC requests to the AFLCMC/GB (WP) Security Office at AFLCMC.HI.WPSecurity@us.af.mil.

8.2.3. Interim Issuance of CAC

Interim issuance of a CAC to a contractor requires the completion of a Federal Bureau of Investigation (FBI) fingerprint check with favorable results and the successful submission of T1 (equivalent or higher) background investigation to the Defense Counterintelligence and Security Agency (DCSA).

8.2.4. Final CAC Determination

A final CAC determination requires a favorably adjudicated T1 (equivalent or higher) investigation based on the basic and supplemental HSPD-12 credentialing standards as outlined in DoDI 5200.46, Enclosures 3 and 4.

8.2.5. Minimum Requirements for Justification

Contractors must maintain the satisfactory minimum requirements for justification of the issuance of a CAC throughout the period of performance.

8.2.6. Termination, Separation, and Expiration of Contract

Contractor personnel shall, within seven calendar days, return all identification badges and/or CAC to the AFLCMC/GB (WP) Security Office upon termination, separation, or expiration of this contract.

8.3. Protection of Information

8.3.1. Controlled Unclassified Information

Controlled Unclassified Information (CUI) is any information that law, regulation, or government-wide policy requires to have safeguarding or disseminating controls. CUI excludes information classified by:

8.3.1.1. Executive Order 13526

Executive Order 13526, *Classified National Security Information*, December 29, 2009

8.3.1.2. Atomic Energy Act of 1954

The Atomic Energy Act of 1954, as amended, or

8.3.1.3. Specific Program or Project Security Classification Guide

A specific program or project Security Classification Guide.

8.3.2. National Archives and Records Administration CUI Registry

The National Archives and Records Administration (NARA) CUI Registry (<http://www.archives.gov/cui/registry/category-list.html>) identifies approved CUI categories and subcategories; provides general descriptions for each; identifies the basis for controls; and sets procedures for the use of CUI.

8.3.3. CUI Guidance

The Contractor shall comply with DoDI 5200.48, *Controlled Unclassified Information*; Department of Defense Manual (DoDM) 5200.01, Volume 1, DoD Information Security Program: Overview, Classification, and Declassification, *Volumes 1, 2, and 3*; and Air Force Guidance Memorandum 2020-16-01, *Air Force Guidance Memorandum for CUI*, 23 July 2020.

8.3.4. Aggregation of Information

The Contractor shall consult the applicable security classification guide to determine if the aggregation of controlled and uncontrolled unclassified information creates a classified document, e-mail, or other communication.

8.3.5. DoDM 5400.07/AFM 33-302

The Contractor shall comply with DoDM 5400.07/Air Force Manual 33-302, *DoD Freedom of Information Act (FOIA) Program*, requirements.

8.3.6. DoDI 8582.01

The Contractor shall protect CUI and unclassified DoD information not approved for public release on non-DoD Information Systems IAW DoDI 8582.01, *Security of Non-DoD Information Systems Processing Unclassified Nonpublic DoD Information*.

8.3.7. NIST Special Publication 800-171

Unless specific categories of CUI require more stringent controls, the Contractor shall protect non-DoD Information Systems using guidelines set forth in NIST Special Publication 800-171, *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations*.

8.3.8. DFARS 252.204-7012

The Contractor shall comply with DFARS 252.204-7012 *Safeguarding Covered Defense Information and Cyber Incident Reporting (Dec 2019)*. This subpart applies to contracts and subcontracts requiring contractors and subcontractors to safeguard covered defense information that resides in or transits through covered contractor information systems. Safeguarding is done by applying specified network security controls. This DFARS subpart also requires reporting of cyber incidents. The subpart does not abrogate any existing contractor physical, personnel, or general administrative security operations governing the protection of unclassified DoD information, nor does it impact requirements of the National Industrial Security Program.

8.4. Operations Security

All contractors whose normal work location is in a DoD/AF facility or on a DoD/AF installation shall comply with OPSEC requirements and training as set forth in DoD Directive 5205.02, *DoD Operations Security Program*, and AFI 10-701, *Operations Security*.

8.5. Information Technology (IT) Level Rating

The contractor shall have the appropriate Information Technology (IT) level rating before performance of duties in support of this contract. Information Technology (IT) Level I, II, and III positions. The IT Level Rating and criteria is described within this section.

- Contractors required to perform system administration, database administration, and/or application administration for all systems within the scope of this PWS *and* who perform administrative tasks via remote access within Defense Information Systems Agency (DISA)-hosted environments shall have IT Level I rating.
- Contractors required to perform software development and limited privileged system access (e.g., User or Application Admins) for all systems within the scope of this PWS shall have IT Level II rating.
- All other contractors not performing a function named above shall have IT Level III rating.

8.5.1. Critical-Sensitive, Information Technology (IT) Level I positions

Those positions in which the incumbent is responsible for the planning, direction, and implementation of a computer security program; major responsibility for the direction, planning and design of a computer system, including the hardware and software; or, can access a system during the operation or maintenance in such a way, and with a relatively high risk for causing grave damage, or realize a significant personal gain.

IT Level I requires a favorably adjudicated Tier 5 investigation, its old equivalent, the Single Scope Background Investigations (SSBI), or their associated reinvestigations. The investigation shall be within scope. Tier 5 and SSBI investigations are within scope if the present date is within six (6) years of the investigation's closing date. If a security clearance is not needed, the contractor may request, though the government program manager, that the government initiate a Tier 5-for-IT-Level I (T5-IT1) investigation.

Criteria for assigning IT Level I:

- Responsible for the development and administration of Agency computer security programs, and also including direction and control of risk analysis and/or threat assessment.
- Significant involvement in life-critical or mission-critical systems.
- Responsible for the preparation or approval of data for input into a system, which does not necessarily involve personal access to the system, but with relatively high risk for effecting grave damage or realizing significant personal gain.
- Relatively high risk assignments associated with or directly involving the accounting, disbursement, or authorization for disbursement from systems of (1) dollar amounts of \$10 million per year or greater, or (2) lesser amounts if the activities of the individual are not subject to technical review by higher authority in the IT Level I category to insure the integrity of the system.
- Positions involving major responsibility for the direction, planning, design, testing, maintenance, operation, monitoring, and/or management of systems hardware and software.
- Other positions as designated by the Agency head that involve relatively high risk for effecting grave damage or realizing significant personal gain.

8.5.2. Non-critical Sensitive, Information Technology (IT) Level II Positions

Those positions in which the incumbent is responsible for the direction, planning, design, operation, or maintenance of a computer system, and whose work is technically reviewed by a higher authority of the IT Level I category to insure the integrity of the system.

IT Level II requires at least a favorably adjudicated Tier 3 investigation, its old equivalent, the National Agency Check with Local Agency Checks and Credit Check (NACLC), or the associated reinvestigations. The investigation shall be within scope. Tier 3 or NACLC investigations are within scope if the present date is within ten (10) years of the investigation's closing date. If a security clearance is not needed, the contractor may request, though the government program manager, that the government initiate a Tier 3-for-IT-Level II (T3-IT2) investigation.

Criteria for assigning IT Level II:

- Responsible for systems design, operation, testing, maintenance, and/or monitoring that is carried out under technical review of higher authority in the IT Level I category, includes, but is not limited to:
 - Access to and/or processing of proprietary data, information requiring protection under the Privacy Act of 1974, and Government-developed privileged information involving the award of contracts;
 - Accounting, disbursement, or authorization for disbursement from systems of dollar amounts less than \$10 million per year. Other positions are designated by the Agency head that involve a degree of access to a system that creates a significant potential for damage or personal gain less than that in IT Level I positions.

8.5.3. Non-sensitive, Information Technology (IT) Level III positions

IT Level III is assigned to all other positions involved in Federal computer activities. IT Level III duties require a favorably adjudicated Tier 1 (T1) background investigation, National Agency Check with Inquiries (NACI) or any higher-level investigation such as the Tier 3 (T3) investigation.

8.5.4. Application & Information System Access Requests

All contractors requiring access to mission or business information systems are required to submit a DD Form 2875, System Authorization Access Control (SAAR) request. Current instructions for completing and uploading a DD Form 2875 can be found through the AFLCMC/GBC Customer Management SharePoint site:

<https://usaf.dps.mil/teams/41319/Network-Account-Requests/Forms/AllItems.aspx>

8.6. Required Security-Related Training

8.6.1. Cyber Awareness Challenge Training

All contractors that requires a DoD or AF network account shall successfully complete Cyber Awareness Challenge (ZZ133098) training. Initial training shall be completed prior to the creation of the network account. This is an annual requirement. Subsequent training must be completed on or before the one-year anniversary of the most recent training completion date. If training is not completed before the one-year anniversary, access to the network account is automatically suspended and not reinstated until proof of training completion is provided.

8.6.2. Force Protection and Anti-Terrorism Training

All contractors whose duty location is in a DoD/AF facility or on a DoD/AF installation successfully complete Force Protection training (ZZ133079). Initial training shall be completed within 30 calendar days of the creation of their AF network account. This is an annual requirement. Subsequent training must be completed on or before the one-year anniversary of the most recent training completion date.

8.6.3. Controlled Unclassified Information Training

All contractors employed under this contract shall successfully complete Controlled Unclassified Information (CUI) training within 30 calendar days of the creation of their AF network account.

8.7. In Processing

8.7.1. In-Processing Checklist

All contractors performing work under this contract shall in-process with AFLCMC/GBC. The government PM or other government POC will create an in-processing checklist and instruct the incoming contract on actions that must be completed.

8.7.2. Visit Requests for Classified Contracts

For classified contracts (i.e. contracts that have a DD254, *Contract Security Classification Specification*), the prime contractor's Facility Security Officer (FSO) shall submit to Security

Management Organization (SMO) Code WE1MFHYN6, via the Defense Information System for Security (DISS), a Visit Request that identifies all contractors that require access to classified information or systems.

8.7.2.1. Contractors Not Requiring Access to Classified Information

The identity of contractors that do not require access to classified information or systems may be submitted on company letterhead stationery (e-mailed pdf document is acceptable). The letter shall include each person's full, legal name; Social Security Number, and employer (to indicate if the person is with the prime- or sub-contractor).

8.7.2.2. WP Security Office Address

The letter shall be addressed to:

AFLCMC/GBC (WP) Security Office
Area A, Bldg. 266, Rm N101
Wright-Patterson AFB, OH 45433-5722
aflcmc.hi.wpsecurity@us.af.mil

8.7.3. Visit Requests for Unclassified Contracts

For unclassified contracts, the prime contractor's FSO, contract manager, or contract task lead shall submit to the AFLCMC/GB (WP) Security Office a visit request that identifies the persons who shall perform work under this contract. The letter may be submitted on company letterhead stationery (e-mailed pdf document is acceptable). The letter shall include each person's full, legal name; Social Security Number, and employer (to indicate if the person is with the prime- or sub-contractor). The letter shall be addressed as shown above.

8.8. Out Processing

8.8.1. Out Processing with AFLCMC/GBC

All contractors performing work under this contract shall out-process with AFLCMC/GBC.

8.8.2. Trusted Associate Sponsorship System (TASS)

Contractors moving to another AF contract may request transfer of CAC sponsorship to the Trusted Associate Sponsorship System (TASS) Trusted Agent (TA) associated with the new contract.

8.8.3. Contractors Ending Association with Air Force/CAC Surrender

Contractors ending their association with the AF shall surrender their CAC to the AFLCMC/GB (WP) Security Office. This may be done in person or, if the contractor is not in the Wright-Patterson AFB vicinity, by mail (e.g., US Postal Service, FedEx, UPS, DHL, etc.).

